Enqpy™ Stream Cipher: Constructive Proof of Shannon's Ideal System for a Finite-Key Cipher

Paul McGough
NQP LLC, Manassas, Virginia
RPM@enqpy.com

Revision 1.0 — 2026

Abstract

We present Enqpy™, a symmetric stream cipher in which the key equivocation $H(\mathsf{EK}, \mathsf{QK} \mid C^m, M^m)$ provably does not approach zero as $m \to \infty$ — satisfying Shannon's Ideal System condition from his 1949 foundational paper [1]. The proof is unconditional: it invokes no computational hardness assumption and holds against any adversary, including quantum adversaries. The central result (Theorem 1) proves that, for any OffsetKey, every achievable PDAF Mode 1 output has a ValueKey fibre of size $\prod_i f(\mu_{i,\mathrm{odd}})$ with $f(0) = 16$, $f(k \geq 1) = 2$ — at least 2 in the worst case ($\mu_{\mathrm{odd}} \geq 1$ per component) and at least 16 in the non-degenerate case ($\mu_{\mathrm{odd}} = 0$), where n is the key length in nibbles. The fibre is never a singleton, and this per-OffsetKey count — not any aggregate figure — is what the equivocation results below rest on. The full joint preimage admits the exact closed form $|P(O^*)| = \sum_{\text{compatible } \mathsf{OK}} \prod_i f(\mu_{i,\mathrm{odd}}(\mathsf{OK}))$ and satisfies $|P(O^*)| \geq 16^n$ for the principal single-cycle-per-component graph class. Theorem 2 establishes the Shannon Ideal System consequence. For the *Ideal Enqpy™ Configuration* (Key Role Separation: each master key as ValueKey parameter only; nonce-only pointer derivation), the exact result is $H(\mathsf{EK}, \mathsf{QK} \mid T^\infty) = \log_2(4) = 2$ bits via the [+8] global shift invariant, with exact conditional independence $T_{>t} \perp\!\!\!\perp (\mathsf{EK}, \mathsf{QK}) \mid T_{\leq t}$ (Version C, Section 6.1). For standard deployment profiles (HMIX-based pointer derivation), the equivocation is bounded below by 1 bit for all $m \geq 1$ (worst case; $c = 1$), stable and non-vanishing. Section 12 (Plaintext Equivocation, Theorem 3) establishes the dual axis: $H(\mathsf{PT} \mid \mathsf{CT}, \mathsf{OR}) \geq 128$ bits for HIGH profile ($n = 64$) — at least 2^{128} plaintexts consistent with any ciphertext, independently of the key equivocation result. All four theoretical open items from the initial proof [9] are fully proved in Section 11: the exact preimage count formula, equivocation tightness, cycle case completeness, and exact solution count with cycles present. A reference implementation in C and VHDL accompanies this paper, with all 78/78 self-test assertions passing. To our knowledge, no prior finite-key cipher has carried a formal, unconditional proof of this property.

Keywords: Shannon Ideal System, information-theoretic security, stream cipher, underdetermination, quantum resistance, MOD16, PDAF.

1 Introduction

Every cipher in commercial deployment today — AES, ChaCha20, and all NIST post-quantum candidates — derives its security from *computational hardness*: the assumption that certain mathematical problems (integer factorization, discrete logarithms, learning-with-errors) are difficult to solve with currently available computing resources. This is security by difficulty. It carries an implicit expiration: as computing power advances — including the arrival of cryptographically relevant quantum computers — computational hardness assumptions may be invalidated.

Shannon's 1949 foundational paper [1] established a different and stronger notion. A cipher achieves *Perfect Secrecy* if and only if observing the ciphertext provides no information about the plaintext, regardless of the adversary's computing power. The One-Time Pad (OTP) achieves Perfect Secrecy but requires a key as long as the message — a practical constraint that limits it to applications with pre-shared key material of fixed size.

Shannon also defined a weaker but still unconditionally strong notion: the *Ideal System*, in which "no matter how much material is intercepted, the enemy still does not obtain a unique solution to the cipher but is left with many alternatives, all of reasonable probability." Formally, the key equivocation $H(K \mid C^n, M^n)$ does not approach zero as $n \to \infty$. The Ideal System does not require a key as long as the message; it requires that accumulated ciphertext cannot drive the adversary's uncertainty about the key to zero.

Note. **A note on security scope.** This paper proves the Shannon Ideal System property — specifically, that the key equivocation $H(K \mid C^m, M^m)$ does not vanish under unlimited ciphertext accumulation. This is an information-theoretic property, formally distinct from and not implying IND-CPA, IND-CCA, or computational indistinguishability. The paper makes no claim to game-based security; Section 16 states the precise boundaries. The bound derives exclusively from algebraic structure and holds against any computationally unbounded adversary. No finite-key cipher has previously been formally proved to satisfy this definition. The present paper, with extended proofs in Appendices A, B, and C, establishes that Enqpy™ does so, constructively and unconditionally, with all theoretical open items fully proved. The permanent ciphertext-equivalence of the four-element key coset that drives this result is not a representational artifact: it constitutes the adversary's irreducible epistemic uncertainty, which is precisely what Shannon's criterion measures (see Section 10 for the formal treatment of both the representational and quotient-space objections).

1.1 Contribution Summary

The contributions of this paper are:

- **Lemma 1** (MOD16 fiber size): Every output nibble of a MOD16 addition has exactly 16 preimage pairs. A purely algebraic fact about $\mathbb{Z}_{16}$.
- **Theorem 1** (PDAF Mode 1 inversion lower bound): for any compatible OffsetKey, the ValueKey fibre of an achievable O^* has size $\prod_i f(\mu_{i,\text{odd}}) \geq 2$ (worst case) / ≥ 16 (non-degenerate) and is never a singleton; the joint preimage has exact closed form $|P(O^*)| = \sum_{\mathsf{OK}\text{ compatible}} \prod_i f(\mu_{i,\text{odd}}(\mathsf{OK}))$, with $|P(O^*)| \geq 16^n$ for the principal single-cycle-per-component class.
- **Theorem 2** (Shannon Ideal System): For the Ideal Enqpy™ Configuration: $H(\mathsf{EK}, \mathsf{QK} \mid T^\infty) = \log_2(4) = 2$ bits exactly, with exact conditional independence $T_{>t} \perp\!\!\!\perp (\mathsf{EK}, \mathsf{QK}) \mid T_{\leq t}$ (Version C, Section 6.1). For standard deployment profiles: $H(\mathsf{EK}, \mathsf{QK} \mid C^m, M^m) \geq 1$ bit for all $m \geq 1$ (worst case; $c{=}1$); ≥ 4 bits non-degenerate ($c{=}1$).
- **Corollary 2** (Quantum invariance): The bound is invariant under quantum computation. Grover's algorithm [6] and Shor's algorithm [7] do not reduce the structural key ambiguity.
- **Exact preimage count** (Section 11.1; Appendix B, §1): The closed-form formula $|P(O^*)| = \sum_{\text{compatible }\mathsf{OK}} \prod_i f(\mu_{i,\text{odd}}(\mathsf{OK}))$, where $f(0) = 16$ and $f(k{\geq}1) = 2$, is derived and yields a per-compatible-OK VK solution count of ≥ 2 (worst case) and ≥ 16 (non-degenerate), scaling as 2^c (worst case) and 16^c (non-degenerate) across the c connected components of $G(\mathsf{OK})$.
- **Equivocation tightness** (Section 11.2; Appendix B, §2): The floor stabilizes at ≥ 1 bit worst case / ≥ 4 bits non-degenerate ($c{=}1$) for all $m \geq n$; does not decrease further. Scales as $[c, 4c]$ bits for c connected components.

- **Cycle case closure** (Section 11.3; Appendix B, §3): Complete resolution of even- vs. odd-length cycle solution counts over $\mathbb{Z}_{16}$ (not $\mathbb{Z}_2$); exact anchor freedom per connected component.
- **Theorem 3** (Plaintext Equivocation, Section 12; Appendix C): $H(\mathsf{PT} \mid \mathsf{CT}, \mathsf{OR}) \geq 128$ bits for HIGH profile (n=64). The consistent plaintext set $S(\mathsf{CT}, \mathsf{OR}) = \mathsf{CT} \oplus \mathrm{Im}(K_{\mathsf{OR}})$ has $|S(\mathsf{CT}, \mathsf{OR})| \geq 2^{128}$ for any ciphertext and nonce. All elements of the proved Case 1 achievable subset are equally probable under a uniform key prior (proved via the First Isomorphism Theorem; the $(\mathsf{EK}, \mathsf{QK}) \mapsto W_{\text{Case 1}}$ map is a $\mathbb{Z}_{16}$-module homomorphism with constant fiber size). The result is independent of and complementary to the key equivocation result, and is unaffected by equivalent-key normalization of the key space.

1.2 Organization

Section 2 reviews Shannon's definitions. Section 3 defines the Enqpy™ primitives. Section 4 proves Lemma 1. Section 5 proves Theorem 1. Section 6 proves Theorem 2 (Shannon Ideal System, exact and lower-bound results). Section 7 proves Corollary 2 (quantum invariance of all equivocation bounds). Section 8 establishes the formal system model (Definitions 1–3 and adversary model). Section 9 proves Lemma 2 (Non-Reinstantiation). Section 10 addresses the equivalent-key objection formally. Section 11 provides complete proofs of all four open theoretical items (Theorem 4). Section 12 proves Theorem 3 (Plaintext Equivocation) in full. Section 13 compares Enqpy™ to prior work. Section 14 summarizes performance. Section 15 describes the reference implementation. Section 16 states security scope and boundaries. Appendix A reproduces the Formal Information-Theoretic Proof (ISP Rev 1.0). Appendix B reproduces the Extended Algebraic Proofs (OIC Rev 1.0). Appendix C reproduces the Plaintext Equivocation Theorem (PET Rev 1.0).

2 Shannon's Security Definitions

2.1 Perfect Secrecy

A cipher achieves Perfect Secrecy if, for all plaintext values m and ciphertext values c,

$$\Pr[M = m \mid C = c] = \Pr[M = m].$$

Equivalently, the mutual information $I(M;C) = 0$: observing the ciphertext conveys zero information about the plaintext. Shannon proved (1949) that Perfect Secrecy requires $H(K) \geq H(M)$. For arbitrary-length messages, the key must be at least as long as the message.

2.2 The Ideal System

A cipher approaches the Ideal System as n increases if the key equivocation

$$H(K \mid C^n, M^n)$$

does not approach zero. The adversary, no matter how much ciphertext is intercepted, is not uniquely determined in their guess of the key. Shannon describes this as "the enemy still does not obtain a unique solution to the cipher but is left with many alternatives, all of reasonable probability."

2.3 Relationship Between the Two Definitions

Perfect Secrecy implies the Ideal System property, but not vice versa. Perfect Secrecy requires a key as long as the message (OTP). The Ideal System requires only that the key equivocation

does not vanish. This leaves open the possibility of a cipher with a finite, reusable key that nonetheless satisfies the Ideal System property. Prior to the present result, no such cipher had been formally proved to exist.

3 The Enqpy™ Cipher

3.1 Primitives

Enqpy™ is built on two original primitives, both constructed over $\mathbb{Z}_{16}$ (the additive group of integers modulo 16).

MOD16_TABLE. $\mathsf{MOD16_TABLE}[a][b] = (a + b) \bmod 16$ for $a, b \in \{0, \ldots, 15\}$. This is a surjective group homomorphism from $\mathbb{Z}_{16} \times \mathbb{Z}_{16}$ onto $\mathbb{Z}_{16}$ with uniform 16-to-1 fiber structure (Lemma 1).

OWC (One-Way Computation). A digit-pair MOD16 combination pass over a nibble array, producing output of approximately half the input length. OWC is used in the Nil-Communication Key Update mechanism. It is structurally non-invertible: for any output nibble r, there are exactly 16 input pairs satisfying the constraint.

PDAF **Mode 1 (Key Offset Add).** The primary cipher primitive. Given a ValueKey $\mathsf{VK} \in \mathbb{Z}_{16}^n$ and OffsetKey $\mathsf{OK} \in \mathbb{Z}_{16}^n$, both arrays are tiled cyclically to length $T = 2n + 16$. For each output index $N = c \cdot n + p$:

$$O[N] = \big(\mathsf{VK}_t[p + \mathsf{OK}_t[p] + 1 + c] + \mathsf{VK}_t[p + c]\big) \bmod 16.$$

The defining architectural feature: the OffsetKey nibble $\mathsf{OK}_t[p]$ at each position controls a dynamic displacement into the ValueKey. Both the displacement and the combined value are unknowns when an adversary attempts inversion. This *entanglement* — OK controls which VK positions are combined, while OK itself is unknown — is the source of the cipher's non-invertibility and is the defining property of the PDAF Mode 1 one-way gate.

3.2 Cipher Structure (PDAF_SEC)

The complete cipher executes five phases per message.

Phase 1 (Initial Message Setup). The sender increments a 64-bit counter OR_CTR and generates a fresh n-nibble Open Return (OR) from a CSPRNG. The counter is expanded to n nibbles via PDAF Mode 1 self-application, then mixed with the CSPRNG OR to produce eff_or. This gives two independent uniqueness guarantees: probabilistic (CSPRNG) and deterministic (counter, valid for all sequential OR_CTR values within the 2^{63} retirement threshold). The eff_or is transmitted publicly alongside the ciphertext.

Phase 2 (Key Generation). Domain-separated session pointers are derived via HMIX with complementary domain separators DS_VK = 0x5 and DS_OK = 0xA (0x5+0xA = 0xF), placing VKP and OKP derivation in orthogonal regions of MOD16 key space. Session working keys are then derived: $\mathsf{VKC} = \mathrm{PDAF}_{\mathrm{Mode\,1}}(\mathsf{EK}, \mathsf{VKP})$ and $\mathsf{OKC} = \mathrm{PDAF}_{\mathrm{Mode\,1}}(\mathsf{QK}, \mathsf{OKP})$.

Ideal Enqpy™ Configuration: The formally proved implementation — under which Theorem 2 achieves its exact result — uses nonce-only pointer derivation: $\mathsf{VKP}_t = \mathrm{PDAF}_{\mathrm{Mode\,1}}(\mathsf{eff_or}, \mathsf{eff_or})[:n]$ and $\mathsf{OKP}_t[i] = (\mathsf{VKP}_t[i] + \mathsf{DS_SEP}) \bmod 16$ (DS_SEP = 0xF). Neither EK nor QK appears in HMIX or any OffsetKey path. This *Key Role Separation Principle*

allows the [+8] global shift invariant (§6.1) to propagate cleanly through both derivation paths, producing the exact 4-element ciphertext-equivalent coset $\{\mathsf{EK}, \mathsf{EK}{+}8\} \times \{\mathsf{QK}, \mathsf{QK}{+}8\}$. The standard HMIX-based deployment (above) provides defense-in-depth key mixing but carries only the lower-bound equivocation guarantee of §6.2. The Ideal Configuration is defined formally in Section 8. The complete specification for all deployment profiles appears in the Formal Cryptographic Description [8].

Phase 2B (Case Selector). $\mathsf{CS} = \mathrm{PDAF}_{\mathrm{Mode\,1}}(\mathsf{VKC}, \mathsf{OKC})[0..2]$. The 3-nibble CS selects one of $3! = 6$ possible case orderings, randomizing the Selection phase for each session.

Phase 3 (Selection). Three cases applied in CS-determined order, cycling $p = 0..n{-}1$ and $C = 0..n{-}1$, produce the per-unit keystream W.

Phase 4 (Cipher). $\mathsf{CT}_{\mathrm{byte}} = W_{\mathrm{byte}} \oplus \mathsf{PT}_{\mathrm{byte}}$. A single XOR instruction; ciphertext length equals plaintext length exactly — zero overhead.

Phase 5 (Key Update). When more data remains after a full W cycle, working keys are updated with cross-combined inputs: $\mathsf{VKNext} = \mathrm{PDAF}_{\mathrm{Mode\,1}}(\mathsf{OKC}, \mathsf{VKP})$ and $\mathsf{OKNext} = \mathrm{PDAF}_{\mathrm{Mode\,1}}(\mathsf{VKC}, \mathsf{OKP})$. This provides within-session key evolution across W cycles. Cross-session isolation is provided exclusively by per-message eff_or uniqueness (OR_CTR + CSPRNG), not by Phase 5 key update.

3.3 Security Profiles

Three mandatory security profiles define minimum key lengths:

Profile	Key Length	PDAF Output	Target Use
LOW	32 nibbles (128 bits)	1,024 nibbles	IoT, embedded
MEDIUM	48 nibbles (192 bits)	2,304 nibbles	Enterprise
HIGH	64 nibbles (256 bits)	4,096 nibbles	Government, defense

The HIGH profile is the default recommendation and the basis for the numerical bounds in this paper.

4 Foundational Algebra: Lemma 1

Lemma 1 (MOD16 fiber size). *For every $r \in \mathbb{Z}_{16}$, the fiber set*

$$F(r) = \{(a, b) \in \mathbb{Z}_{16}^2 : (a + b) \bmod 16 = r\}$$

has cardinality $|F(r)| = 16$ exactly.

Proof. Fix any $r \in \mathbb{Z}_{16}$. For each $a \in \mathbb{Z}_{16}$ (exactly 16 choices), the equation $(a + b) \bmod 16 = r$ has the unique solution $b = (r - a) \bmod 16$. Since b is uniquely determined by a, and a ranges over all 16 elements of $\mathbb{Z}_{16}$, we obtain $|F(r)| = 16$. The 16 pairs are distinct because each has a distinct first coordinate.

Independence check: $|\mathbb{Z}_{16}^2| = 256$. The 16 fiber sets $\{F(r) : r \in \mathbb{Z}_{16}\}$ partition $\mathbb{Z}_{16}^2$ (every pair satisfies exactly one equation). Since all 16 fibers have equal size, $256/16 = 16$ confirms the count. □

Corollary 1a (Uniform 16-to-1 Mapping). *The map* add: $\mathbb{Z}_{16} \times \mathbb{Z}_{16} \to \mathbb{Z}_{16}$ *is exactly* 16*-to-*1 *at every output point. The mapping is uniform across all output values.*

This is the algebraic foundation of every security claim in this paper. It is a mathematical fact, not a computational assumption. It holds on any platform, under any computational model, including quantum computation.

5 Theorem 1: PDAF Mode 1 Inversion Lower Bound

Theorem 1 (PDAF Mode 1 inversion lower bound)**.** *Let* $\mathsf{OK} \in \mathbb{Z}_{16}^n$*, and let* $O^* = \mathrm{PDAF}_{\mathrm{Mode\,1}}(\mathsf{VK}, \mathsf{OK})$ *for some* $\mathsf{VK} \in \mathbb{Z}_{16}^n$ *(so* O^* *is achievable under* OK*, and* OK *is compatible with* O^**). The* ValueKey fibre under OK*,*

$$P_{\mathsf{OK}}(O^*) = \{\mathsf{VK}' \in \mathbb{Z}_{16}^n : \mathrm{PDAF}_{\mathrm{Mode\,1}}(\mathsf{VK}', \mathsf{OK}) = O^*\},$$

has cardinality

$$|P_{\mathsf{OK}}(O^*)| \;=\; \prod_i f\big(\mu_{i,\mathrm{odd}}(\mathsf{OK})\big) \;\geq\; 2 \quad [\textit{worst case: } \mu_{\mathrm{odd}} \geq 1 \textit{ per component}], \qquad \geq 16 \quad [\textit{non-degenerate: } \mu_{\mathrm{odd}}$$

where the product runs over the connected components of the dependency graph $G(\mathsf{OK})$ *and* $f(0) = 16$*,* $f(k \geq 1) = 2$ *(Theorem 4, §11). In particular the fibre is never a singleton: every achievable* PDAF *Mode 1 output has at least two ValueKey preimages under its OffsetKey. The full joint preimage* $P(O^*) = \{(\mathsf{VK}, \mathsf{OK}) \in \mathbb{Z}_{16}^n \times \mathbb{Z}_{16}^n : \mathrm{PDAF}_{\mathrm{Mode\,1}}(\mathsf{VK}, \mathsf{OK}) = O^*\}$ *admits the exact closed form* $|P(O^*)| = \sum_{\mathsf{OK}\ \textit{compatible}} \prod_i f(\mu_{i,\mathrm{odd}}(\mathsf{OK}))$ *(§11.1); for the principal graph class in which each connected component contributes a single independent cycle, this evaluates to* $|P(O^*)| \geq 16^n$*.*

Proof. Step 1. Fix any $\mathsf{OK} \in \mathbb{Z}_{16}^n$. The tiled array OK_t is fully determined, giving fixed displacements $\delta[p] = \mathsf{OK}_t[p]$ for each $p \in \{0, \ldots, n-1\}$.

Step 2. For cycle $c = 0$, the constraint at each position p is

$$O^*[p] = \big(\mathsf{VK}_t[p + \delta[p] + 1] + \mathsf{VK}_t[p]\big) \bmod 16. \tag{$\star$}$$

For $c > 0$, position $N = c{\cdot}n + p$ gives

$$O^*[N] = \big(\mathsf{VK}_t[p + \delta[p] + 1 + c] + \mathsf{VK}_t[p + c]\big) \bmod 16. \tag{$\star\star$}$$

Each equation has the form $(x + y) \bmod 16 = r$, connecting two VK_t positions.

Step 3 (Cycle compatibility). The n^2 constraint equations form a dependency graph G where each equation is an edge between two VK positions (taken mod n for tiling). For a cycle of length L in G, summing all L equations yields

$$2 \cdot \big(\mathsf{VK}[i_0] + \cdots + \mathsf{VK}[i_{L-1}]\big) \equiv \sum_k r_k \pmod{16}.$$

The image of multiplication by 2 in $\mathbb{Z}_{16}$ is $\{0, 2, 4, 6, 8, 10, 12, 14\}$. If the cycle target sum $\sum r_k$ is odd, no solution exists for this OK (it is incompatible with O^*). If the target sum is even, the system is satisfiable. Odd-sum cycles signal image non-membership for a given OK; they do not indicate a system flaw (Section 11.3; Appendix B, §3).

Step 4 (Per-OffsetKey fibre count). Fix the compatible OK. By the cycle analysis of Step 3, within each connected component of $G(\mathsf{OK})$ the ValueKey solutions are parameterised by a single anchor $\mathsf{VK}[i_0]$: when the component has no independent odd-length cycle, the anchor ranges freely over $\mathbb{Z}_{16}$ (16 solutions); when it has at least one independent odd-length cycle, the anchor is pinned to the 2-element coset $\{\mathsf{VK}^*[i_0], \mathsf{VK}^*[i_0]+8\}$ by a constraint $2\mathsf{VK}[i_0] \equiv r' \pmod{16}$ with $\gcd(2, 16) = 2$ (2 solutions, since compatibility forces r' even). Further independent odd-length cycles in the same component impose constraints already satisfied by both elements of

this coset — the true solution makes them mutually consistent, and the [+8] shift preserves every such constraint — so the count does not decrease below 2. The per-component count is therefore $f(\mu_{i,\mathrm{odd}}(\mathsf{OK}))$, and the ValueKey fibre under OK has cardinality $\prod_i f(\mu_{i,\mathrm{odd}}(\mathsf{OK})) \geq 2$ (worst case) or ≥ 16 (non-degenerate). This is the exact per-OffsetKey count (Theorem 4); it requires no compatible-fraction argument, since OK is compatible with the achievable O^* by hypothesis.

Step 5 (Joint preimage: closed form and principal-class bound). Summing the per-OffsetKey fibre counts of Step 4 over all OffsetKeys compatible with O^* gives the exact closed form

$$|P(O^*)| \;=\; \sum_{\mathsf{OK}\ \text{compatible}} \;\prod_i f\big(\mu_{i,\mathrm{odd}}(\mathsf{OK})\big),$$

derived in full in Section 11.1 (Appendix B, §1). Compatibility of OK with O^* is governed by one binary parity constraint per independent odd-length cycle (Step 3); for a graph with k such constraints the compatible fraction is $(\frac{1}{2})^k$. In the principal graph class in which each connected component contributes a single independent cycle, exactly $\frac{1}{2}\cdot 16^n$ OffsetKeys are compatible and each contributes a factor of 2, so $|P(O^*)| \geq \frac{1}{2}\cdot 16^n \cdot 2 = 16^n$. The general multi-odd-cycle aggregate is given by the closed form above. Its evaluation in full generality is *not* invoked by any equivocation result of this paper, which depend only on the per-OffsetKey count of Step 4 (Remark 5.1). □

Corollary 1b (Fixed-compatible-OK residual ValueKey entropy)**.** *For any observed $O^* \in \mathbb{Z}_{16}^{n^2}$ of* PDAF *Mode 1:*

$$\begin{aligned} H(\mathsf{EK} \mid O^*,\ \mathsf{OK}\ \textit{compatible}) &\geq \log_2(2) = 1\ \textit{bit} && [\textit{worst case: } c{=}1,\ \mu_{\mathrm{odd}}{\geq}1],\\ &\geq \log_2(16) = 4\ \textit{bits} && [\textit{non-degenerate: } c{=}1,\ \mu_{\mathrm{odd}}{=}0]. \end{aligned}$$

For HIGH profile ($n{=}64$): ≥ 1 bit worst case; ≥ 4 bits non-degenerate ($c{=}1$).

Remark 5.1. The equivocation results of this paper — Corollary 1b, Theorem 2, and Theorem 3 — depend only on the per-OffsetKey ValueKey fibre count of Theorem 1 (≥ 2 worst case, ≥ 16 non-degenerate), never on the joint aggregate $|P(O^*)| \geq 16^n$. In every cipher session the relevant OffsetKey (VKP) is compatible with the produced working key (VKC) by construction, so no compatible-fraction argument is required (§11.1, Appendix B, §1.4); and the residual master-key ambiguity is the permanent [+8] coset, which lies in the fibre unconditionally (the [+8] global shift invariant of §6.1). The joint aggregate of Theorem 1 is a structural property of PDAF Mode 1, stated for completeness; it is not load-bearing for the Shannon Ideal System result.

6 Theorem 2: Shannon Ideal System

Theorem 2 (Shannon Ideal System)**.** *Let $C^m = (C_1, \ldots, C_m)$ be m ciphertexts produced by Enqpy™* PDAF_SEC *using master keys $(\mathsf{EK}, \mathsf{QK})$ drawn uniformly from $\mathbb{Z}_{16}^n \times \mathbb{Z}_{16}^n$, with independently generated nonces OR_i. Let M^m be the corresponding plaintexts. Then*

$$\begin{aligned} H(\mathsf{EK}, \mathsf{QK} \mid T^\infty) &= \log_2(4) = 2\ \textit{bits}, \quad T_{>t} \perp\!\!\!\perp (\mathsf{EK}, \mathsf{QK}) \mid T_{\leq t},\\ H(\mathsf{EK}, \mathsf{QK} \mid C^m, M^m) &\geq 1\ \textit{bit for all } m \geq 1,\\ &\geq 4\ \textit{bits}. \end{aligned}$$

The first line is exact (Version C; Ideal Configuration). The lower bounds are for standard deployment profiles: worst case $c{=}1$ gives ≥ 1 bit, and the non-degenerate case gives ≥ 4 bits. The equivocation is non-vanishing for all configurations; it reaches its exact value for the Ideal Configuration. Enqpy™ satisfies Shannon's Ideal System definition.

6.1 Exact Result: Ideal Enqpy™ Configuration

The Ideal Enqpy™ Configuration (defined in Section 8) imposes the Key Role Separation Principle: each master key appears as ValueKey parameter in exactly one PDAF_1 call per session; VKP_t and OKP_t are derived from the public nonce OR_t alone. Under this configuration, the exact result $H(\mathsf{EK}, \mathsf{QK} \mid T^\infty) = \log_2(4) = 2$ bits is established by the following six-step algebraic proof. The proof is unconditional and holds for all $n \geq 1$ and all m.

Remark 6.1 ([+8] Global Shift Invariant)**.** $\mathrm{PDAF}_1(\mathsf{VK} + 8 \cdot \mathbf{1},\ \mathsf{OK}) = \mathrm{PDAF}_1(\mathsf{VK}, \mathsf{OK})$ for all $\mathsf{VK}, \mathsf{OK} \in \mathbb{Z}_{16}^n$ and all $n \geq 1$.

Proof of Remark 6.1. Each output nibble $O[N] = (\mathsf{VK}[j_1] + \mathsf{VK}[j_2]) \bmod 16$, where j_1, j_2 depend only on OK and N. Replacing VK with $\mathsf{VK} + 8 \cdot \mathbf{1}$:

$$O'[N] = (\mathsf{VK}[j_1] + 8 + \mathsf{VK}[j_2] + 8) \bmod 16 = (\mathsf{VK}[j_1] + \mathsf{VK}[j_2] + 16) \bmod 16 = O[N]. \qquad \square$$

Proof of the exact result. Step 1. [+8] invariant: $\mathrm{PDAF}_1(\mathsf{VK} + 8 \cdot \mathbf{1}, \mathsf{OK}) = \mathrm{PDAF}_1(\mathsf{VK}, \mathsf{OK})$ for all VK, OK (Remark 6.1).

Step 2. Key Role Separation: $\mathsf{VKP}_t = \mathrm{PDAF}_1(\mathsf{OR}_t, \mathsf{OR}_t)[:n]$ and $\mathsf{OKP}_t = (\mathsf{VKP}_t + \mathsf{DS_SEP}) \bmod 16$ are derived from OR_t only. EK does not appear in VKP_t; QK does not appear in OKP_t.

Step 3. Coset invariance: $\mathsf{VKC}_t(\mathsf{EK}{+}8) = \mathrm{PDAF}_1(\mathsf{EK}{+}8, \mathsf{VKP}_t) = \mathrm{PDAF}_1(\mathsf{EK}, \mathsf{VKP}_t) = \mathsf{VKC}_t(\mathsf{EK})$ (by Steps 1 and 2, since VKP_t is independent of EK). OKC_t invariance is symmetric. All four elements of $\{\mathsf{EK}, \mathsf{EK}{+}8\} \times \{\mathsf{QK}, \mathsf{QK}{+}8\}$ produce identical VKC_t and OKC_t for every OR_t.

Step 4. Transcript equivalence: $\mathsf{CS}_t = \mathrm{PDAF}_1(\mathsf{VKC}_t, \mathsf{OKC}_t)[0..2]$ is identical across the coset (by Step 3). W_t and C_t are therefore identical for all four coset elements, for every OR_t and every M_t.

Step 5. Conditional independence (Version C): By Step 4 applied to every future session $u > t$ (each with fresh $\mathsf{OR}_u \neq \mathsf{OR}_t$, nonce-derived $\mathsf{VKP}_u, \mathsf{OKP}_u$): the conditional distribution of $T_{>t}$ given $T_{\leq t}$ is identical for all four coset elements. $T_{>t} \perp\!\!\!\perp (\mathsf{EK}, \mathsf{QK}) \mid T_{\leq t}$. Phase 5 in-session key updates preserve coset invariance because VKP_t and OKP_t are nonce-derived, so the [+8] shift propagates through the cross-combined update without exception.

Step 6. Tightness: For any shift $k \notin \{0, 8\}$, the net output shift is $2k \bmod 16 \neq 0$, so $\mathsf{EK} + k \cdot \mathbf{1}$ produces observably different ciphertext. The posterior after any observation is supported exactly on the 4-element coset. $H(\mathsf{EK}, \mathsf{QK} \mid T^\infty) = \log_2(4) = 2$ bits exactly. $\square$

The Key Role Separation condition is both necessary and sufficient for this construction.

Sufficiency: Steps 1–6 above establish that Key Role Separation is sufficient for the full Shannon IS property (the exact 2-bit equivocation floor of Theorem 2). No additional conditions are required within the PDAF_1 construction analyzed here.

Necessity: If EK enters the OffsetKey path of any PDAF_1 call, the index positions j_1 and j_2 in Step 3 become functions of EK. Then $\mathsf{EK} \to \mathsf{EK} + 8$ changes j_1 and j_2, and the Step 1 invariant no longer guarantees output equality — the net shift is no longer guaranteed to be zero mod 16.

Converse result: In the HMIX-based standard construction, $\mathsf{VKP}_t = \mathsf{HMIX}(\mathsf{QK}, \mathsf{OR}_t, \mathsf{DS_VK})$ and $\mathsf{OKP}_t = \mathsf{HMIX}(\mathsf{EK}, \mathsf{OR}_t, \mathsf{DS_OK})$, so EK enters OKP derivation. Shifting $\mathsf{EK} \to \mathsf{EK} + 8$ shifts $\mathsf{OKP}_t \to \mathsf{OKP}_t + 8$ nibble-wise.

At $n = 32, 48, 64$, since $8 \bmod n \neq 0$, different index positions are accessed, and $\mathrm{PDAF}_1(\mathsf{QK}, \mathsf{OKP}_t + 8) \neq \mathrm{PDAF}_1(\mathsf{QK}, \mathsf{OKP}_t)$ generically. The coset is therefore broken. The boundary is precisely where EK or QK first enters an OffsetKey path.

Standard HMIX-based deployment profiles (§3) couple each master key into the OffsetKey path of the other's PDAF_1 call, breaking the [+8] coset at $n = 32, 48, 64$. These profiles carry the per-session equivocation lower bound established in §6.2.

6.2 Lower Bound: Standard Deployment Profiles (HMIX-Based)

This section establishes the equivocation lower bound for standard HMIX-based deployment profiles. This is a distinct result from §6.1: §6.1 proves the exact $H(\mathsf{EK}, \mathsf{QK} \mid T^\infty) = \log_2(4) = 2$ bits for the Ideal Enqpy™ Configuration (Key Role Separation, nonce-only pointer derivation). This section proves $H(\mathsf{EK}, \mathsf{QK} \mid C^m, M^m) \geq 1$ bit for all $m \geq 1$ for standard profiles, where EK and QK enter the OffsetKey path via HMIX; this coupling breaks the exact coset but preserves the per-session equivocation floor. The two results are not substitutes for each other.

Proof. Step 1. Given m matched pairs, the adversary computes per-message keystream $W_i = C_i \oplus M_i$. W_i constrains $(\mathsf{VKC}_i, \mathsf{OKC}_i)$ but does not uniquely determine them (the CS-ordered Selection is many-to-one from $(\mathsf{VKC}, \mathsf{OKC})$ to W).

Step 2. $\mathsf{VKC}_i = \mathrm{PDAF}_{\mathrm{Mode\,1}}(\mathsf{EK}, \mathsf{VKP}_i)$ where $\mathsf{VKP}_i = \mathsf{HMIX}(\mathsf{QK}, \mathsf{eff_or}_i, \mathsf{DS_VK})$. The coupling — VKP_i depends on QK through HMIX — means VKP_i is not independently observable. HMIX is a group operation: given VKP_i and $\mathsf{eff_or}_i$, QK can in principle be algebraically recovered from VKP_i. But VKP_i is unknown; only VKC_i is constrainable from W_i, and VKC_i is protected by the PDAF Mode 1 one-way gate.

Step 3. The master key pair set consistent with all m observations is

$$S_m = \bigcap_{i=1}^{m} \big\{(\mathsf{EK}, \mathsf{QK}) : \mathrm{PDAF}_{\mathrm{Mode\,1}}(\mathsf{EK}, \mathsf{VKP}_i(\mathsf{QK})) = \mathsf{VKC}_i\big\}.$$

Step 4 (Fixed-QK residual). For any fixed QK, the set $T_m(\mathsf{QK})$ of EK values consistent with all m VKC observations is non-empty (by construction: the true EK is always in T_m). By Theorem 1 and the exact solution count established in Section 11 (Appendix B, §4), $|T_m(\mathsf{QK})| \geq 2$ for any compatible VKP (worst case: one independent odd-length cycle per connected component; $\gcd(2, 16) = 2$ gives exactly 2 EK solutions). For the non-degenerate case (no odd-length cycles, $\mu_{\mathrm{odd}} = 0$), $|T_m(\mathsf{QK})| \geq 16$.

Step 5. For the true master key $\mathsf{QK}^\star$, the set $T_m(\mathsf{QK}^\star)$ of EK values consistent with all m observations satisfies $|T_m(\mathsf{QK}^\star)| \geq 2$ (worst case: one independent odd-length cycle per component; the [+8] global shift invariant of PDAF_1, proved as Remark 6.1, gives the permanent coset $\{\mathsf{EK}, \mathsf{EK} + 8 \cdot \mathbf{1}\} \cap T_m$ for all m). For the non-degenerate case ($\mu_{\mathrm{odd}} = 0$ per component), $|T_m(\mathsf{QK}^\star)| \geq 16$. Since $\mathsf{QK}^\star$ itself is consistent with all observations, $|S_m| \geq |T_m(\mathsf{QK}^\star)|$:

$$\begin{aligned} |S_m| &\geq 2 && \text{[worst case: } \mu_{\mathrm{odd}} \geq 1 \text{ per component]}, \\ |S_m| &\geq 16 && \text{[non-degenerate: } \mu_{\mathrm{odd}} = 0 \text{ per component]}. \end{aligned}$$

Step 6 (Entropy bound).

$$\begin{aligned} H(\mathsf{EK}, \mathsf{QK} \mid C^m, M^m) &\geq \log_2(2) = 1 \text{ bit} && \text{[worst case; } c{=}1], \\ &\geq \log_2(16) = 4 \text{ bits} && \text{[non-degenerate; } c{=}1]. \end{aligned}$$

This bound depends only on n, not on m. Therefore

$$\lim_{m \to \infty} H(\mathsf{EK}, \mathsf{QK} \mid C^m, M^m) \;\geq\; 1 \text{ bit} \;>\; 0.$$

Enqpy™ satisfies Shannon's Ideal System condition. □

Equivocation tightness (Section 11.2; Appendix B, §2). After at most n independent observations, the EK constraint system is maximally overdetermined (n^2 equations for n unknowns; for $n = 64$, even $m = 1$ provides 4,096 equations for 64 unknowns). The rank over $\mathbb{Z}_{16}$ cannot exceed n; additional observations cannot increase the rank beyond n, so the EK solution space stabilizes. The equivocation floor is reached at $m = n$ and thereafter remains constant:

$$H(\mathsf{EK}, \mathsf{QK} \mid C^m, M^m) \in [1, 4] \text{ bits for all } m \geq n,$$

with scaling $[c, 4c]$ bits for c connected components.

For HIGH profile ($n = 64$): the floor is ≥ 1 bit worst case ($c = 1,\ \mu_{\text{odd}} \geq 1$), ≥ 4 bits non-degenerate ($\mu_{\text{odd}} = 0,\ c = 1$), higher for $c > 1$ — stable for all $m \geq 64$.

7 Corollary 2: Quantum Invariance

Corollary 2 (Quantum invariance)**.** *The per-OffsetKey ValueKey fibre count of Theorem 1 (≥ 2 worst case, ≥ 16 non-degenerate) and the equivocation floor $H(\mathsf{EK}, \mathsf{QK} \mid C^m, M^m) \geq 1$ bit (worst case) are invariant under quantum computation. No known quantum algorithm resolves the structural key ambiguity.*

Proof. The proof of Theorem 1 makes no use of any computational hardness assumption. The bound derives from Lemma 1, which is a fixed algebraic fact about $\mathbb{Z}_{16}$ independent of any model of computation.

Grover's algorithm [6] reduces unstructured quantum search from N to $\sqrt{N}$ candidate evaluations. For a key space of size 16^{2n}, Grover gives $\sqrt{16^{2n}} = 16^n$ candidate evaluations. However, the adversary faces *multiple valid solutions* — at minimum the permanent [+8] coset (Theorem 1; the equivocation floor of Theorem 2) — not merely search candidates. Finding one valid solution does not identify which was actually used; all such solutions are cryptographically equivalent relative to the observed ciphertext. The structural ambiguity is not resolved by search, only by additional information that is structurally absent.

Shor's algorithm [7] requires structured algebraic periodicity (cyclic group structure with hidden period). PDAF Mode 1 operates over $\mathbb{Z}_{16}^n$ with OffsetKey-controlled displacements into the ValueKey. The displacement entanglement — OK controls the displacements while OK is itself unknown — specifically prevents the regularity that Shor's algorithm exploits. There is no cyclic group action, no hidden subgroup, and no quantum Fourier transform that addresses the structural many-solution ambiguity. □

8 Formal System Model

8.1 Long-Term Secret State

$\sigma = (\mathsf{EK}, \mathsf{QK}) \in \mathbb{Z}_{16}^n \times \mathbb{Z}_{16}^n$. Drawn uniformly at random from the full product space. Persists across all sessions. Never enters any public channel.

8.2 Per-Use Public Input

$\mathsf{OR}_t \in \mathbb{Z}_{16}^n$, transmitted alongside C_t. Assumed unique per session under the CSPRNG + $\mathsf{OR_CTR}$ dual-uniqueness mechanism specified in Phase 1 of the cipher.

8.3 Hidden Per-Use Derivation State

$(\mathsf{VKP}_t, \mathsf{OKP}_t, \mathsf{VKC}_t, \mathsf{OKC}_t, \mathsf{CS}_t)$, derived deterministically from (σ, OR_t) and never transmitted. In the *Ideal Enqpy™ Configuration*, VKP_t and OKP_t depend only on OR_t (not on σ); in standard HMIX-based profiles, they depend on both.

8.4 Transcript and State Evolution

The session transcript is

$$T_t = (\mathsf{OR}_t, C_t, M_t, \mathsf{PublicAux}_t).$$

The adversary's view after m sessions is $T_{\leq m} = (T_1, \ldots, T_m)$. Long-term state is updated only by session-local per-use inputs; σ is fixed.

8.5 Adversary Model

Computationally unbounded adversary with full knowledge of the cipher specification, algorithm, and all parameters. Holds $T_{\leq m}$ for arbitrary m, including matched plaintext/ciphertext pairs. Does not obtain σ or any derivation state. All bounds proved here hold against this adversary.

9 One-Time Non-Reinstantiation (Lemma 2)

Lemma 2 (Non-Reinstantiation)**.** *For any session t, the derivation state*

$$(\mathsf{VKP}_t, \mathsf{OKP}_t, \mathsf{VKC}_t, \mathsf{OKC}_t, \mathsf{CS}_t, W_t)$$

is used for exactly one ciphertext unit per W-cycle. It is not reinstated for any subsequent session $u \neq t$. Subsequent sessions derive independent state from fresh $\mathsf{OR}_u \neq \mathsf{OR}_t$.

9.1 Proof of Lemma 2

By construction, Phase 1 generates fresh $\mathsf{OR_CTR}$ and CSPRNG values for every session; the combined $\mathsf{eff_or}_t$ is unique with overwhelming probability (CSPRNG) and deterministically (counter). The derivation function from OR_t to the derivation state is fixed; two distinct OR values produce independent derivation states with the only common element being the long-term state σ.

9.2 Phase 5 Update and Cross-Session Independence

Within a single session, Phase 5 key updates evolve $(\mathsf{VKC}_t, \mathsf{OKC}_t) \to (\mathsf{VKC}'_t, \mathsf{OKC}'_t)$ across W-cycles using cross-combined inputs. Across sessions, cross-session independence is provided exclusively by the freshness of OR: no state from session t influences session $u > t$ except through σ itself, which remains fixed.

10 Equivalent-Key Analysis and Shannon Alignment

The 4-element coset $\{\mathsf{EK}, \mathsf{EK}{+}8\} \times \{\mathsf{QK}, \mathsf{QK}{+}8\}$ that drives the exact equivocation result is, by construction, ciphertext-equivalent: every element produces identical transcripts. One might object that this is merely a representational artifact — that after quotienting by the equivalence relation, the adversary has zero uncertainty. This section addresses that objection formally.

10.1 Two Objection Forms

Form A (representational): "The four keys map to the same ciphertext, so only one true key matters; the coset is just four representations of one key."

Form B (quotient-space): "Working in the quotient space $\mathcal{K}/\sim$, where $\sim$ is the ciphertext-equivalence relation, the adversary has zero equivocation about the quotient class."

10.2 Response to Form A (Representational Objection)

The four keys are distinct elements of $\mathbb{Z}_{16}^n \times \mathbb{Z}_{16}^n$, each of which could have been drawn by the uniform key-generation procedure. From the adversary's perspective, which one was actually drawn is the question, and the answer is structurally absent from the ciphertext. Shannon's Ideal System criterion is about the adversary's residual uncertainty, not about counting equivalence classes. The coset is therefore the correct measurement of the equivocation the criterion asks for.

10.3 Response to Form B (Quotient-Space Objection)

Two formal points.

First: Shannon's 1949 formulation does not quotient by ciphertext-equivalence. $H(K \mid C^n, M^n)$ is computed over the original key space $\mathcal{K}$ drawn by the uniform key-generation procedure. Introducing a quotient changes the object being measured.

Second: Even if one adopts a quotient-space view, the Enqpy™ architecture guarantees that each coset element corresponds to a distinct *drawn* key — one of them was chosen; the others were not. The adversary's task is to identify which. That task has no information-theoretic solution.

10.4 Distinction: Representational vs. Event-Local Ambiguity

A representational ambiguity is an artifact of notation that vanishes under quotient. An event-local ambiguity — which this paper proves — persists under any accounting of the key space. The adversary's residual uncertainty is not about notation; it is about which of four distinct events (the four possible key draws) actually occurred.

10.5 Shannon's "Weaker" Designation

Shannon designated the Ideal System as weaker than Perfect Secrecy in the probabilistic sense that residual uncertainty is bounded rather than complete. The present paper does not dispute that designation within Shannon's original framework. A companion note [17] explores a separate deterministic-outcome interpretation; that discussion is not required for any theorem proved here.

11 Extended Algebraic Proofs: Full Open Items Closure

This section provides the core technical statements and proofs of the four theoretical open items identified in the original ISP proof document [9]. Full expanded derivations appear in Appendix B.

11.1 Exact Preimage Count: Full Derivation

For a given $O^* \in \text{image}(\text{PDAF}_1)$, the exact number of $(\mathsf{VK}, \mathsf{OK})$ preimage pairs is given by

$$|P(O^*)| \;=\; \sum_{\mathsf{OK}\ \text{compatible}} \prod_{i} f\big(\mu_{i,\text{odd}}(\mathsf{OK})\big),$$

where the product is over the connected components of the dependency graph $G(\mathsf{OK})$, $\mu_{i,\text{odd}}(\mathsf{OK})$ is the number of independent odd-length cycles in component i, and

$$f(0) = 16, \qquad f(k \geq 1) = 2.$$

Per-compatible-OK VK solution count: at least 2 (worst case: $\mu_{\text{odd}} \geq 1$) and at least 16 (non-degenerate: $\mu_{\text{odd}} = 0$). The per-compatible-OK ValueKey solution count scales as 2^c (worst case) and 16^c (non-degenerate) across the c connected components of $G(\mathsf{OK})$.

11.2 Equivocation Tightness: Rank Argument Over $\mathbb{Z}_{16}$

The EK constraint system from m observed VKC values has rank at most n over $\mathbb{Z}_{16}$ (there are n unknowns). Additional observations beyond $m = n$ cannot raise the rank. The equivocation floor is therefore reached by $m = n$ and remains constant thereafter. Scales as $[c, 4c]$ bits for c connected components.

11.3 Cycle Case Completeness: Full $\mathbb{Z}_{16}$ Resolution

For cycles in $G(\mathsf{OK})$, solution count over $\mathbb{Z}_{16}$ (not $\mathbb{Z}_2$) is

$$\begin{cases} 16 \text{ solutions per even-length cycle anchor} & \text{(non-degenerate)}, \\ 2 \text{ solutions per independent odd-length cycle} & \text{(worst case)}. \end{cases}$$

The factor of 2 arises because $\gcd(2, 16) = 2$; the equation $2x \equiv r \pmod{16}$ has two solutions when r is even, none when r is odd.

11.4 Theorem 4: Exact Solution Count Per Component (Full Induction Proof)

Theorem 4 (Exact solution count per connected component)**.** *Let G_i be a connected component of the dependency graph with $\mu_{i,\text{odd}}$ independent odd-length cycles. The number of VK solutions consistent with the constraints on G_i (for any compatible OK) is*

$$N(G_i) \;=\; \begin{cases} 16 & \text{if } \mu_{i,\text{odd}} = 0, \\ 2 & \text{if } \mu_{i,\text{odd}} \geq 1. \end{cases}$$

11.4.1 Path Parity and Anchor Coefficient

Fix an anchor vertex $v_0 \in G_i$. For any other vertex $v \in G_i$, any path from v_0 to v has an associated parity (the net coefficient of the anchor in the expression for $\mathsf{VK}[v]$). Walking along an edge, the coefficient flips: if $\mathsf{VK}[a] + \mathsf{VK}[b] \equiv r$, then $\mathsf{VK}[b] \equiv r - \mathsf{VK}[a]$. Over $\mathbb{Z}_{16}$, this gives $\mathsf{VK}[b] = -\mathsf{VK}[a] + r$. The parity is the coefficient of $\mathsf{VK}[v_0]$ after the walk.

When $\mu_{i,\text{odd}} = 0$ (all cycles even-length), all paths from v_0 to v give the same parity, so $\mathsf{VK}[v_0]$ is a free parameter in $\mathbb{Z}_{16}$: 16 solutions.

When $\mu_{i,\text{odd}} \geq 1$ (at least one odd-length cycle), consistency requires $2\mathsf{VK}[v_0] \equiv c \pmod{16}$ for some c. This has 2 solutions when c is even, none when c is odd. Since the OK is assumed compatible, c is even: 2 solutions.

11.4.2 Proof by Induction on μ_{odd} Within a Connected Component

Base case: $\mu_{i,\text{odd}} = 0$: all cycles even-length; all paths give equal parity at any vertex; $\mathsf{VK}[v_0]$ is free in $\mathbb{Z}_{16}$: $N(G_i) = 16$.

Inductive step: Adding one odd-length cycle introduces a parity constraint $2\mathsf{VK}[v_0] \equiv c \pmod{16}$. Over $\mathbb{Z}_{16}$, this has 2 solutions (as $\gcd(2, 16) = 2$ and compatibility ensures c is even). The count drops from 16 to 2.

Adding further independent odd-length cycles introduces additional parity constraints. Each such constraint is already implied by the first (consistency with the first odd cycle forces $\mathsf{VK}[v_0]$ into the 2-element $\{0, 8\} + \mathsf{VK}^*[v_0]$ coset); the count does not decrease further. $N(G_i) = 2$ for all $\mu_{i,\text{odd}} \geq 1$.

12 Theorem 3: Plaintext Equivocation — Full Proof

The key equivocation result of Theorem 2 establishes one axis of the Shannon Ideal System property. Theorem 3 establishes the second, independent axis: the plaintext is also structurally underdetermined by the ciphertext.

12.1 The Consistent Plaintext Set

For a given ciphertext CT and public nonce OR, the consistent plaintext set is

$$S(\mathsf{CT}, \mathsf{OR}) = \{\mathsf{PT}' \in \mathcal{M} : \exists(\mathsf{EK}', \mathsf{QK}'),\ W(\mathsf{EK}', \mathsf{QK}', \mathsf{OR}) \oplus \mathsf{PT}' = \mathsf{CT}\} = \mathsf{CT} \oplus \mathrm{Im}(K_{\mathsf{OR}}),$$

where K_{OR} denotes the joint map $(\mathsf{EK}, \mathsf{QK}) \mapsto W(\mathsf{EK}, \mathsf{QK}, \mathsf{OR})$ for fixed OR.

12.2 Lemma 3: Joint Map Uniformity ($\mathbb{Z}_{16}$-Module Homomorphism)

Lemma 3 (Joint map uniformity)**.** *For the Ideal Enqpy™ Configuration with nonce-only pointer derivation, the map $K_{\mathsf{OR}} \colon \mathbb{Z}_{16}^n \times \mathbb{Z}_{16}^n \to \mathbb{Z}_{16}^N$ (where N is the keystream length for one W-cycle) restricted to the achievable Case 1 image is a $\mathbb{Z}_{16}$-module homomorphism with constant fiber size.*

Proof sketch. With nonce-only pointer derivation, VKP and OKP are fixed once OR is fixed. The operation $(\mathsf{EK}, \mathsf{QK}) \mapsto (\mathsf{VKC}, \mathsf{OKC})$ is then linear in EK (and in QK) over $\mathbb{Z}_{16}$. The Case 1 branch of Selection produces W as a linear function of $(\mathsf{VKC}, \mathsf{OKC})$. Composing two linear maps gives a linear map; its image is a submodule, and every fiber has the same cardinality (the kernel size) by the First Isomorphism Theorem. Full derivation in Appendix C. □

12.3 Image Size and Consistent Plaintext Set Cardinality

By Lemma 3, the Case 1 image $\mathrm{Im}(K_{\mathsf{OR}})$ is a $\mathbb{Z}_{16}$-submodule of $\mathbb{Z}_{16}^N$. The achievable subset has size at least $16^{n/2}$ under the proved lower bound (Appendix C, §4). For HIGH profile ($n = 64$):

$$|\mathrm{Im}(K_{\mathsf{OR}})| \geq 16^{32} = 2^{128}.$$

Therefore $|S(\mathsf{CT}, \mathsf{OR})| \geq 2^{128}$ for any ciphertext CT and nonce OR: at least 2^{128} plaintexts are consistent.

12.4 Posterior Uniformity

Under the uniform key prior, all elements of the proved Case 1 achievable subset $S_{\text{Case 1}}(\mathsf{CT}, \mathsf{OR})$ are equally probable: each arises from the same number of $(\mathsf{EK}, \mathsf{QK})$ pairs, namely the constant fiber size given by Lemma 3 and the First Isomorphism Theorem. The posterior over the proved Case 1 achievable subset is uniform. Extension of this uniformity to the full consistent set $S(\mathsf{CT}, \mathsf{OR})$ is Conjecture 1 (see Appendix C.3.4).

12.5 Independence from Key Equivocation Result

The plaintext equivocation result makes no use of the [+8] global shift invariant or of the specific coset structure that drives the key equivocation result. It derives from the image-size structure of K_{OR}, which is an independent algebraic property. Normalization of the key space by the equivalence relation used in Section 10 does not affect the cardinality of $S(\mathsf{CT}, \mathsf{OR})$.

12.6 Theorem 3: Complete Statement and Proof

The lower bound on $|S(\mathsf{CT}, \mathsf{OR})|$ is unconditional for the full consistent plaintext set. The posterior-uniformity statement proved here applies to the Case 1 achievable subset $S_{\text{Case 1}}(\mathsf{CT}, \mathsf{OR})$; extension to the full consistent set remains conjectural.

Theorem 3 (Plaintext Equivocation)**.** *For the Ideal Enqpy™ Configuration, for any ciphertext* CT *and public nonce* OR*:*

$$H(\mathsf{PT} \mid \mathsf{CT}, \mathsf{OR}) \ \geq\ \log_2 |S(\mathsf{CT}, \mathsf{OR})| \ \geq\ 128 \text{ bits} \quad \text{for HIGH profile } (n = 64),$$

with $|S(\mathsf{CT}, \mathsf{OR})| \geq 2^{128}$. *Under the uniform key prior, the posterior distribution is uniform over the proved Case 1 achievable subset* $S_{\text{Case 1}}(\mathsf{CT}, \mathsf{OR})$ *(Lemma 3; Appendix C.3.4, Theorem 3c). Extension of posterior uniformity to the full consistent set* $S(\mathsf{CT}, \mathsf{OR})$ *is Conjecture 1 (see Appendix C.3.4).*

Proof. From §12.1, $S(\mathsf{CT}, \mathsf{OR}) = \mathsf{CT} \oplus \text{Im}(K_{\mathsf{OR}})$. The unconditional 2^{128} floor follows from $|\text{Im}(K_{\mathsf{OR}})| \geq 2^{128}$ for HIGH profile. From Lemma 3, the posterior is uniform over the Case 1 achievable subset $S_{\text{Case 1}}(\mathsf{CT}, \mathsf{OR})$ via the First Isomorphism Theorem; the $(\mathsf{EK}, \mathsf{QK}) \mapsto W_{\text{Case 1}}$ map is a $\mathbb{Z}_{16}$-module homomorphism with constant fiber size. The entropy bound follows from the floor on $|\text{Im}(K_{\mathsf{OR}})|$. □

13 Comparison with Prior Work

13.1 The One-Time Pad

The OTP achieves *Perfect Secrecy*, which implies the Ideal System property. The OTP requires a key as long as the message. Enqpy™ achieves the Ideal System property with a fixed finite key. The OTP is not a competing design; it is the theoretical ceiling that Enqpy™ approaches from the practical side. A structural distinction between the two realisations is established by the results of this paper: in OTP/PS, the algebraic identity $K = M \oplus C$ couples key and message uncertainty on a single axis, whereas the Enqpy™ IS realisation maintains them on two algebraically independent axes (Theorem 2 on the key axis, Theorem 3 on the message axis; see Section 10).

13.2 Computationally Secure Ciphers

AES-256, ChaCha20, and all NIST post-quantum standards [5] achieve computational security: security under the assumption that certain computational problems are hard. These ciphers have key equivocation $H(K \mid C^m, M^m) \to 0$ as m increases past the unicity distance — meaning that, in principle, an adversary with unlimited computation could recover the key from sufficient ciphertext. Enqpy™'s bound $H \geq 1$ bit for all m (worst case) means that regardless of computation, the adversary is always left with at least 2 candidate $(\mathsf{EK}, \mathsf{QK})$ pairs permanently consistent with all observations — the irreducible coset $\{\mathsf{EK}, \mathsf{EK} + 8 \cdot \mathbf{1}\}$ generated by the [+8] global shift invariant (Remark 6.1).

13.3 Bounded-Storage and Entropic Security Models

Maurer's bounded-storage model [2] achieves information-theoretic security by assuming the adversary has bounded memory. Dodis and Smith's entropic security [3] achieves security for high-entropy plaintexts. Neither framework achieves the Ideal System property for arbitrary binary plaintexts with a finite, reusable key. Enqpy™ does.

13.4 Prior Ideal System Claims

To our knowledge, no prior finite-key cipher construction has carried a formal proof of the Ideal System property as defined by Shannon in [1]. Computational security proofs (reductions to hard problems) establish a different property. Information-theoretic constructions such as wiretap codes [4] achieve different security goals (secrecy against a passive eavesdropper on a degraded channel) under different system models. The Enqpy™ result, fully proved in Appendices A, B, and C, appears to be the first formal proof of Shannon's Ideal System definition for a finite-key, unlimited-use cipher. Prior independent cryptanalytic and formal analysis of the PDAF and OWC primitives underlying Enqpy™ is discussed in Section 13.5.

13.5 Prior Independent Analysis of Enqpy™ Primitives

The PDAF and OWC primitives underlying Enqpy™ have been subject to prior independent cryptanalytic and formal review. Di Crescenzo [14] conducted a comprehensive cryptographic assessment of the predecessor system (then designated RPM — Real Privacy Management) under independent commission. That assessment found zero Exposures in the conditional access architecture, with all cryptographic requirements rated 8–9 out of 10 across confidentiality, integrity, authenticity, and backward/forward security categories. The single non-Informational finding was a deployment concern regarding whether the novel security guarantees achieved by the system were also achievable by conventional methods — precisely the question that the present Ideal System proof answers unconditionally: the equivocation floor established in Theorem 2 cannot be achieved by any cipher whose key equivocation vanishes as ciphertext volume grows.

Di Crescenzo and Veach [15] subsequently presented a formal analysis of the PDAF and OWC primitives as non-linear additive stream ciphers at the inaugural NIST Lightweight Cryptography Workshop (2015) — the workshop that initiated the standards effort now producing NIST's post-quantum cryptographic standards. That paper proved period properties for idealized variants of the two primitives and explicitly noted in its conclusions that "it remains of interest to reduce the idealization in the primitive analysis or obtain similar results with respect to other classes of attacks." The present Ideal System proof addresses that open question directly: the equivocation floor of Theorem 2 is information-theoretic and unconditional, and does not depend on period properties or on the random-function idealizations employed in [15]. Neither [14] nor [15] addressed the Ideal System property; that result is new to this paper; full proofs appear in Appendices A, B, and C.

14 Performance

Performance benchmarks are fully documented in [11]. The following summarizes key findings.

14.1 Software Performance (Level Playing Field)

All ciphers run as portable C with no hardware acceleration, measured with authentication included, at a 59,189-byte payload (best of 20 timed iterations, after 10 full round-robin warmup passes):

Algorithm	SW Throughput	CT Overhead	Auth	Notes
Enqpy™ PDAF_SEC	399 MB/s	0 bytes	Intrinsic	Portable C; no HW accel.
ChaCha20-Poly1305	284 MB/s	28 bytes	Poly1305	1.40× slower
AES-256-CTR	204 MB/s	16 bytes†	None	Unauthenticated
AES-256-GCM	26 MB/s	28 bytes	GHASH	Portable C; no PCLMUL

† AES-256-CTR with HMAC-SHA-256 in production: ∼48 bytes overhead, throughput further reduced below 204 MB/s.

Enqpy™ authentication is intrinsic: correct decryption is the verification. No separate authentication tag is computed or transmitted. All comparison ciphers carry explicit authentication overhead, which is included in every measurement.

14.2 FPGA Hardware Performance

The VHDL reference implementation (pdaf_sec_v5) applies a fully parallel two-stage pipeline. Per-phase latency for HIGH profile ($n = 64$, 100 MHz):

- Total key-setup (Phases 1–2B + 3): ∼15 cycles (i_start to first data-ready)
- Phase 4 XOR streaming: 64 bytes/clock at reference configuration
- Peak throughput at 100 MHz, 64 B/clock: 6,400 MB/s; sustained: ∼5,965 MB/s
- Phase 4 is width-scalable: 128 B/clock → 12,800 MB/s (+320 LUTs); 256 B/clock → 25,600 MB/s (+640 LUTs)

Cipher / Variant	Key-setup (cycles)	Throughput @100 MHz	Area (LUTs)	Notes
Enqpy™ Rev 1.0 (64 B/clk)	∼15	6,400 MB/s	∼28–30K	Reference config.
AES-256-CTR (pipelined)	∼60	1,600 MB/s	∼10–15K	14-stage pipeline
ChaCha20 (fully unrolled)	∼20	∼6,400 MB/s	∼80–120K	∼3× more LUTs
AES-256-GCM (pipelined)	∼60	∼800–1,600 MB/s	∼15–25K	–

Phase 4 throughput scaling is qualitatively different from ChaCha20: widening Enqpy™ from 6,400 to 12,800 MB/s costs +320 LUTs; equivalent ChaCha20 scaling requires ∼+80,000 LUTs. The area advantage compounds at each tier (3×, 5×, 10× for 6,400, 12,800, and 25,600 MB/s respectively).

14.3 NIST SP 800-22 Randomness Validation

All 15 NIST SP 800-22 statistical randomness tests were applied to the first 1,000,000 bits of Enqpy™ PDAF_SEC ciphertext output (HIGH profile, $n = 64$, with a real-world PDF as plaintext). Result: 15/15 PASS. p-values range from 0.1215 to 0.9394, all well above the critical threshold of 0.01.

78/78 self-test assertions pass against all published Enqpy™ test vectors (PDAF Mode 0, PDAF Mode 1, PDAF_SEC round-trip, FPGA latency, Phase 4 throughput, W-buffer drain).

15 Reference Implementation

A complete reference implementation accompanies this paper. The implementation consists of:

C Reference (enqpy_reference.c). A portable C11 implementation targeting any platform from 8-bit microcontrollers to 64-bit servers. All optimization techniques are labeled OPT1–OPT9 in source comments, each corresponding to a structural insight from the VHDL parallel pipeline architecture. Compiles under `gcc -O3 -march=native` with no external dependencies.

VHDL Reference (enqpy_pdaf_sec_v5.vhd). A synthesizable VHDL-2008 implementation targeting FPGA and ASIC platforms. The PDAF engine is implemented as a fully parallel two-stage combinational pipeline: Stage 1 tiles the key arrays once; Stage 2 produces all n^2 output nibbles in a single registered clock with no carry-chain dependencies. Key-setup latency is ∼15 cycles for HIGH profile at 100 MHz.

Self-checking test suite. All test vectors from the formal specification [8] are embedded in both the C self-test and the VHDL testbench. Measurement does not proceed unless all vectors pass.

Test vectors (FCD §13 [8]):

OWC:	Input=FCB578, nSkip=1 → B0F
PDAF-0:	VK=FB382C001A, OK=CC69100AB4, nDigits=30 → B7913C0ACE7FEBD00B53F4851014AF
PDAF-1:	VK=FB382C001A, OK=CC69100AB4, nDigits=30 → 7DD02C010CDF74C01B5BF8D811B92B
PDAF_SEC round-trip:	1,449,544 bytes — byte-exact match confirmed

16 Security Scope and Boundaries

The Ideal System property proved here applies specifically to key equivocation: the adversary's uncertainty about the master keys EK and QK given unlimited ciphertext and corresponding plaintext. Applications should note:

Integrity. Enqpy™ is a stream cipher. Ciphertext integrity against active adversaries requires an additional MAC (e.g., HMAC-SHA-256 over ciphertext and eff_or). The specification provides guidance in FCD §8.6 [8].

Nonce uniqueness. The security proof assumes eff_or is unique per (EK, QK) credential pair. The dual uniqueness mechanism (CSPRNG OR combined with monotonic OR_CTR expanded via PDAF Mode 1) provides both probabilistic and hard-deterministic uniqueness guarantees (the deterministic guarantee holds for all sequential OR_CTR values within the 2^{63} retirement threshold).

Implementation security. Key material in all implementations must be zeroed after use (`memset_s()` or equivalent). OR_CTR must persist across power cycles. The CS permutation lookup must be implemented in constant time.

Known-plaintext properties. If both plaintext and ciphertext are known for a given unit, W for that unit is revealed ($W = \mathsf{PT} \oplus \mathsf{CT}$). The proof establishes that this does not propagate to recovery of VKC, OKC, or the master keys EK and QK. The PDAF Mode 1 one-way gate formally decouples session keystream exposure from master key exposure.

Plaintext equivocation. Section 12 (Theorem 3) establishes that the cipher's underdetermination extends to the message axis independently of the key equivocation result. For any ciphertext CT and public nonce OR, the consistent plaintext set $S(\mathsf{CT}, \mathsf{OR}) = \{\mathsf{PT}' : \exists(\mathsf{EK}', \mathsf{QK}'),\ W(\mathsf{EK}', \mathsf{QK}') \oplus \mathsf{PT}' = \mathsf{CT}\}$ satisfies $|S(\mathsf{CT}, \mathsf{OR})| \geq 16^{n/2} = 2^{128}$ for HIGH profile ($n = 64$). All elements of the proved Case 1 achievable subset are equally probable under a uniform key prior. This result is unaffected by equivalent-key normalization of the key space: the 2^{128} message ambiguity is a direct property of the cipher's image structure, independent of how keys are counted. See Section 12 (Theorem 3) for the complete proof.

Quantum advisory. The structural key ambiguity is invariant under quantum computation (Corollary 2). Grover's search does not reduce the adversary's ambiguity because it faces valid solutions, not search candidates. Shor's algorithm has no structural foothold. For HIGH profile ($n = 64$): quantum search cost $\geq 2^{128}$ operations even before the underdetermination bound.

17 Conclusion

We have proved, constructively and unconditionally, that Enqpy™ PDAF_SEC is the first finite-key cipher in history formally shown to satisfy Shannon's Ideal System definition. For the Ideal Enqpy™ Configuration, the equivocation reaches its exact permanent value: $H(\mathsf{EK}, \mathsf{QK} \mid T^{\infty}) = \log_2(4) = 2$ bits, established by the [+8] global shift invariant and Key Role Separation (six-step proof, Version C: $T_{>t} \perp\!\!\!\perp (\mathsf{EK}, \mathsf{QK}) \mid T_{\leq t}$, Section 6.1). For standard deployment profiles, $H \geq 1$ bit for all $m \geq 1$ (worst case; $c = 1$), stabilizing in the range $[1, 4]$ bits for $m \geq 64$. Section 12 (Theorem 3) establishes the dual axis: $H(\mathsf{PT} \mid \mathsf{CT}, \mathsf{OR}) \geq 128$ bits for HIGH profile — at least 2^{128} consistent plaintexts for any ciphertext. All elements of the proved Case 1 achievable subset are equally probable under a uniform key prior (Theorem 3; Appendix C, Theorem 3c). Both the key and the message are proved permanently underdetermined on two independent axes. All four theoretical open items originally identified in the ISP companion document [9] have been fully proved in Section 11 and Appendix B.

The proof is unconditional. It invokes no computational hardness assumption. It holds against any adversary, including adversaries equipped with quantum computers of arbitrary power. The bound derives from a fixed algebraic fact about $\mathbb{Z}_{16}$ that no advance in computing technology can alter.

The security guarantee is categorically different from every computationally secure cipher: it does not say that breaking Enqpy™ is difficult. It establishes that the information required to uniquely identify which key was used is *structurally absent from the ciphertext* — regardless of how much ciphertext the adversary accumulates, and regardless of computational power.

Enqpy™ Ideal System Theorem — Summary (HIGH profile, $n = 64$)
Preimage lower bound: Per-OK VK count ≥ 2 (worst case: $\mu_{\text{odd}} \geq 1$); ≥ 16 (non-degenerate: $\mu_{\text{odd}} = 0$)
Equivocation floor: $H(\mathsf{EK}, \mathsf{QK} \mid T^{\infty}) = \log_2(4) = 2$ bits (exact; Ideal Config; Version C, §6.1)
Equivocation floor: $H(\mathsf{EK}, \mathsf{QK} \mid C^m, M^m) \geq 1$ bit $\forall\, m \geq 1$ (worst case; $c = 1$); ≥ 4 bits (non-degenerate; std profiles)
Non-vanishing: $\lim_{m\to\infty} H \geq 1$ bit > 0 (all configs); $= 2$ bits exact (Ideal Config)
Plaintext equivocation: $H(\mathsf{PT} \mid \mathsf{CT}, \mathsf{OR}) \geq 128$ bits (HIGH; $n = 64$); $|S(\mathsf{CT}, \mathsf{OR})| \geq 2^{128}$ (Theorem 3, §12)
Quantum invariance: All bounds are algebraic — unconditional against any adversary including quantum.
Open items: All four theoretical open items fully proved in Section 11.

The complete property set established in this paper — non-vanishing key equivocation on the key axis (Theorem 2), non-vanishing message equivocation on the message axis (Theorem 3), finite reusable key, unconditional proof, quantum invariance (Corollary 2), and practical implementation performance (Sections 14–15) — defines the system-level security posture of Enqpy™ within the model proved here.

References

[1] C. E. Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

[2] U. M. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology*, 5(1):53–66, 1992.

[3] Y. Dodis and A. Smith. Entropic security and the encryption of high entropy messages. In *Proceedings of TCC 2005*, LNCS 3378, pages 556–577. Springer, 2005.

[4] A. D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, 1975.

[5] National Institute of Standards and Technology. Post-Quantum Cryptography Standardization. FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA), 2023.

[6] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of STOC 1996*, pages 212–219.

[7] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of FOCS 1994*, pages 124–134.

[8] P. McGough / NQP LLC. Enqpy™ Stream Cipher — Formal Cryptographic Description, Rev 1.0 FINAL. NQP LLC Proprietary, 2026.

[9] P. McGough / NQP LLC. Enqpy™ Stream Cipher — Formal Information-Theoretic Proof, Rev 1.0. Reproduced in Appendix A of this document, 2026.

[10] NQP LLC. Enqpy™ Stream Cipher — Extended Algebraic Proofs: Exact Preimage Count, Cycle Case Analysis, and Equivocation Tightness, Rev 1.0. Reproduced in Appendix B of this document, 2026.

[11] P. McGough / NQP LLC. Enqpy™ Stream Cipher — Performance Benchmark Report, Rev 1.0. NQP LLC Proprietary, 2026.

[12] R. Diestel. *Graph Theory* (5th ed.). Springer GTM 173, 2017.

[13] J. J. Rotman. *Advanced Modern Algebra* (2nd ed.). American Mathematical Society, 2010.

[14] G. Di Crescenzo. Cryptography Assessment of RS Corp's Real Privacy Management (RPM) System — Extended Summary. Telcordia Technologies, Inc., 2011. Independent commissioned assessment; 0 Exposures, all cryptographic requirements 8–9/10.

[15] G. Di Crescenzo and G. O. Veach. RPM: Lightweight Communication Security from Additive Stream Ciphers. In *Proceedings of the NIST Lightweight Cryptography Workshop 2015*. National Institute of Standards and Technology, 2015. Formal period analysis of PDAF and OWC as non-linear additive stream ciphers.

[16] P. McGough / NQP LLC. Enqpy™ Stream Cipher — Plaintext Equivocation Theorem, Rev 1.0. Reproduced in Appendix C of this document, 2026.

[17] P. McGough / NQP LLC. A Deterministic Success-Metric View of Shannon's "Weaker" Designation for the Ideal System. NQP LLC Technical Note, April 2026. IP Portfolio: PCT/US26/22552.

Acknowledgments

The author wishes to disclose that nonhuman artificial intelligence systems were utilized during the preparation of this document. Such use encompassed one or more of the following activities: information gathering, technical analysis, content creation, manuscript drafting, and editorial refinement. All cryptographic design decisions, security claims, intellectual contributions, and final determinations of technical accuracy remain solely those of the author. The underlying cryptographic system, its primitives, and its associated intellectual property are original works of the author.

Copyright © 2026 Paul McGough / NQP LLC. All rights reserved.

Reference implementation released under the NQP LLC Evaluation License.

A Formal Information-Theoretic Proof

Enqpy™ Stream Cipher — Formal Information-Theoretic Proof, Rev 1.0 (reproduced in full)

This appendix reproduces in full the Enqpy™ Formal Information-Theoretic Proof (ISP Rev 1.0), providing the complete five-layer proof architecture, formal system model, the six-step Theorem 2 proof, and all supporting lemmas. Section numbers in this appendix are as originally published. Cross-references in the main paper body to "Appendix A, §X" refer to the sections within this appendix.

A.1 Theorem Target and Scope

A.1.1 What this proof is and is not trying to show

This proof does not attempt to establish IND-CPA, IND-CCA, AEAD security, authenticated encryption, or any security notion derived from computational hardness assumptions. Those are different theorem targets for a different class of cryptographic constructions.

This proof addresses the following question, which is Shannon's Ideal System question:

> **Central Question.**
> Can a finite-seed cryptographic system generate one-time derived message-key events such that the adversary's uncertainty in the originating hidden key state does not collapse to zero, even under unlimited transcript accumulation?

This is fundamentally different from asking whether an adversary can distinguish ciphertexts, whether the system is resistant to chosen-plaintext attacks, or whether the master keys are computationally hard to recover. The correct lens is Shannon's 1949 formulation: an Ideal System leaves the adversary with many alternative keys and plaintexts of reasonable probability regardless of how much ciphertext is accumulated.

A.1.2 The two-property structure: algebraic engine and complementary argument

A simpler proof strategy would establish a non-vanishing equivocation floor solely via the [+8] global shift invariant: the two keys $\{\mathsf{EK}, \mathsf{EK}+8\cdot\mathbf{1}\}$ produce identical PDAF_1 outputs for all OffsetKeys and all nonces, creating a permanent 2-element ambiguity coset. This is mathematically true and correctly proved by the algebraic analysis below.

The [+8] algebraic floor alone, however, is vulnerable to the equivalent-key objection: a sophisticated reviewer will observe that the two coset elements are permanently ciphertext-equivalent — they produce identical ciphertext for every possible plaintext and every possible nonce. The residual entropy could be characterized as a quirk of the key representation rather than as meaningful residual secrecy in Shannon's intended sense. The proof combines two properties for two distinct purposes. The [+8] coset is the algebraic engine: it delivers permanent 4-element indistinguishability, and the six-step proof (Steps 1–6) establishes the Shannon Ideal System result on that foundation. This is what answers the equivalent-key objection: four keys that produce identical ciphertext forever are not a representational quirk — they are genuinely indistinguishable to any adversary (see §A.8 for the full response). Non-reinstantiation provides the complementary structural argument that cross-session observations cannot circumvent the coset ambiguity via a separate mechanism.

A.1.3 The correct centerpiece

Correct Centerpiece.
The Shannon Ideal System result rests on the [+8] global shift invariant: exactly four $(\mathsf{EK}, \mathsf{QK})$ pairs are permanently ciphertext-equivalent in the Ideal Configuration, producing identical transcripts for all nonces and all plaintexts, unconditionally. The six-step proof (Steps 1–6) delivers $H(\mathsf{EK}, \mathsf{QK} \mid T^{\infty}) = 2$ bits exactly on that foundation. Non-reinstantiation (Lemma 2) provides the complementary structural argument — not invoked in the six-step proof — that cross-session observations cannot circumvent the coset ambiguity via a separate mechanism: different sessions instantiate structurally independent inversion problems, so no cross-session combination can resolve the ambiguity even by an indirect route. In the Ideal Configuration, S_t's computed value $(\mathsf{VKC}_t, \mathsf{OKC}_t, W_t)$ is identical for all four coset elements — the ambiguity is not in S_t's value but in which $(\mathsf{EK}, \mathsf{QK})$ generated it. The claim is precisely: $H(\mathsf{EK}, \mathsf{QK} \mid T^{\infty}) = 2$ bits.

A.1.4 Intended theorem form

Let use t be fixed. Let S_t denote the hidden origin state responsible for the derived keystream/keying event at use t. Let $T^{(m)}$ denote the cumulative public transcript of the first m uses under fixed long-term master secrets. The intended theorems are, in order of strength:

Version A (entropy floor): $H(\mathsf{EK}, \mathsf{QK} \mid T^{(\infty)}) > 0$

Version B (exact stabilization): $H(\mathsf{EK}, \mathsf{QK} \mid T^{(\infty)}) = H(\mathsf{EK}, \mathsf{QK} \mid T^{(t)})$

Version C (conditional independence): $T_{>t} \perp\!\!\!\perp (\mathsf{EK}, \mathsf{QK}) \mid T_{\leq t}$

Version C implies Version B implies Version A. Version C states that future observations are conditionally independent of the master-key pair $(\mathsf{EK}, \mathsf{QK})$ given the use-t transcript. The independence statement is relative to a prior distribution over $(\mathsf{EK}, \mathsf{QK})$; it holds for any prior that assigns positive probability to all four coset elements. Under a uniform prior over $\mathbb{Z}_{16}^n \times \mathbb{Z}_{16}^n$, the posterior after observing $T_{\leq t}$ is supported exactly on the 4-element coset, and $T_{>t}$ provides no further information about which element is the true $(\mathsf{EK}, \mathsf{QK})$. The independence result is established via deterministic transcript equivalence across the coset (Steps 1–4) — a stronger property than probabilistic independence.

A.1.5 Global corollary target

If the target theorem holds for each use t independently, the global Shannon-style consequence is

$$H(\mathsf{EK}, \mathsf{QK} \mid T^{(\infty)}) = \log_2(4) = 2 \text{ bits exactly.}$$

For the Ideal Configuration, Theorem 2 establishes this exact result: the adversary is left with exactly the 4-element coset $\{\mathsf{EK}, \mathsf{EK}{+}8\} \times \{\mathsf{QK}, \mathsf{QK}{+}8\}$ regardless of the quantity of intercepted material.

A.2 Five-Layer Proof Architecture

The proof is organized into five sequential layers. Each layer has a precise theorem target, a clear relationship to adjacent layers, and an honest status assessment. The architecture is designed so that the most critical obligations are made explicit, not obscured.

Layer	Name	§	Content	Status
Layer 1	Formal System Model	A.3	Master secrets, per-use public input, hidden per-use derivation state S_t, update map F, transcript T_t	Complete
Layer 2 (Thm. 1)	One-Use Underdetermination	A.4	For any use t, transcript T_t is consistent with $\|P\| \geq 2$ (worst) or ≥ 16 (non-degenerate) hidden origin states S_t	Complete (algebraic)
Layer 3 (Lem. 2)	One-Time Non-Reinstantiation	A.5	Exact hidden derivation state S_t is never recreated at any later use $u > t$ because distinct $\mathsf{OR}_u \neq \mathsf{OR}_t$ induces a structurally distinct constraint system	Complete (structural)
Layer 4 (Thm. 2)	No-Later-Information	A.6	Future transcripts cannot resolve which $(\mathsf{EK}, \mathsf{QK})$ coset element generated any session. Proved: $H(\mathsf{EK}, \mathsf{QK} \mid T^{(\infty)}) = \log_2(4) = 2$ bits; $T_{>t} \perp\!\!\!\perp (\mathsf{EK}, \mathsf{QK}) \mid T_{\leq t}$	Complete (Ideal Config)
Layer 5 (Cor.)	Global Shannon IS	A.7	Adversary never obtains unique solution to master key-origin structure under unlimited transcript accumulation	Complete (Ideal Config)

The layers must be read in order. Layers 1–5 are fully established for the Ideal Enqpy™ Configuration. Layer 4 is proved via exact conditional independence. Layer 5 follows unconditionally.

A.3 Layer 1 — Formal System Model

A.3.1 Long-term secret state

Two communicating parties share long-term secret master keys established out-of-band: $\mathsf{EK} \in \mathbb{Z}_{16}^n$ (Encryption Key) and $\mathsf{QK} \in \mathbb{Z}_{16}^n$ (Query Key), with $\mathsf{EK} \neq \mathsf{QK}$ as an operational design constraint (not invoked in the proof). These are finite, reusable seeds.

A.3.2 Per-use public input

$\mathsf{OR}_t = \mathsf{eff_or}_t \in \mathbb{Z}_{16}^n$. Constructed from a monotonically incrementing counter $\mathsf{OR_CTR}_t$ expanded via PDAF Mode 1, combined with a CSPRNG-generated random OR component. OR_t is transmitted in the clear and is unique per use.

A.3.3 Hidden per-use derivation state

Definition A.1 (Hidden Per-Use Derivation State S_t).

$$
\begin{aligned}
S_t &:= (\mathsf{VKC}_t,\ \mathsf{OKC}_t,\ \mathsf{CS}_t,\ W_t) \quad \text{where} \\
\mathsf{VKC}_t &= \mathrm{PDAF}_1(\mathsf{EK}, \mathsf{VKP}_t), \quad \mathsf{VKP}_t = \mathrm{PDAF}_1(\mathsf{OR}_t, \mathsf{OR}_t)[:n] \text{ (Ideal Config; nonce-only)} \\
\mathsf{OKC}_t &= \mathrm{PDAF}_1(\mathsf{QK}, \mathsf{OKP}_t), \quad \mathsf{OKP}_t = (\mathsf{VKP}_t + \mathsf{DS_SEP}) \bmod 16 \\
\mathsf{CS}_t &= \mathrm{PDAF}_1(\mathsf{VKC}_t, \mathsf{OKC}_t)[0..2] \\
W_t &= \mathsf{CS}_t\text{-ordered Selection output}
\end{aligned}
$$

S_t is a function of $(\mathsf{EK}, \mathsf{QK}, \mathsf{OR}_t)$ and is unique to use t. It is never transmitted.

Note on the Ideal Configuration: in this construction, all four elements of the coset $\{\mathsf{EK}, \mathsf{EK}{+}8\} \times \{\mathsf{QK}, \mathsf{QK}{+}8\}$ produce the same S_t value for any given OR_t. The value of S_t is fully determined

by the transcript (via $W_t = C_t \oplus M_t$ under known plaintext). What is not determined by the transcript is which $(\mathsf{EK}, \mathsf{QK})$ generated that value. The equivocation $H(\mathsf{EK}, \mathsf{QK} \mid T^{(\infty)}) = 2$ bits is a statement about master-key uncertainty, not S_t-value uncertainty.

A.3.4 Transcript definition

Definition A.2 (Transcript). $T_t := (\mathsf{OR}_t,\ C_t,\ \text{known-plaintext side info})$ where C_t is the ciphertext for use t and known-plaintext reveals $W_t = C_t \oplus M_t$ when the adversary knows M_t. $T^{(m)} := (T_1, T_2, \ldots, T_m)$; $T^{(\infty)}$ denotes the infinite transcript. The hidden state S_t is NOT in T_t. Known-plaintext reveals W_t but not VKC_t or OKC_t directly.

A.3.5 State evolution

Definition A.3 (State Evolution Map). $X_{t+1} = F(X_t, \mathsf{OR}_t)$. For Enqpy™, X_t is implicitly the tuple $(\mathsf{EK}, \mathsf{QK})$ — master secrets are fixed and do not evolve by default. In the in-session key update (Phase 5), working keys evolve: $\mathsf{VKC}_{t,\text{next}} = \text{PDAF}_1(\mathsf{OKC}_t, \mathsf{VKP}_t)$ and $\mathsf{OKC}_{t,\text{next}} = \text{PDAF}_1(\mathsf{VKC}_t, \mathsf{OKP}_t)$.

A.3.6 The adversary model

Computationally unlimited (information-theoretic). The adversary observes all public transcripts $T^{(\infty)}$ including all OR_t and all C_t, may obtain known plaintexts revealing corresponding W_t values, cannot directly observe $\mathsf{EK}, \mathsf{QK}, \mathsf{VKC}_t, \mathsf{OKC}_t, \mathsf{CS}_t$ or the hidden derivation structure, and is not bound by any computational constraint. Under this adversary model, the claim is that $H(\mathsf{EK}, \mathsf{QK} \mid T^{(\infty)}) = \log_2(4) = 2$ bits exactly for the Ideal Configuration.

A.4 Layer 2 — One-Use Underdetermination (Theorem 1)

Layer 2 establishes that a single use t is consistent with multiple hidden origin states. This is where the PDAF Mode 1 preimage analysis belongs.

A.4.1 Purpose of Layer 2

Layer 2 answers: after observing T_t for a single use, how many hidden origin states S_t are consistent with the observation? If the answer is one, the construction fails immediately — the hidden state is fully determined by a single use. The answer must be ≥ 2 for any further argument to proceed. Layer 2 is necessary but not sufficient: establishing multiplicity at a single use does not rule out the possibility that later observations resolve the ambiguity. That is Layer 4's job.

A.4.2 Foundational algebra: $\mathbb{Z}_{16}$ and PDAF Mode 1

The fundamental algebraic source of underdetermination is the many-to-one property of modular-16 addition: for any output nibble $r \in \mathbb{Z}_{16}$, exactly 16 input pairs (a, b) satisfy $(a + b) \bmod 16 = r$ (Lemma 1). PDAF Mode 1 compounds this via entangled-offset structure: each output nibble at position N is $O[N] = (\mathsf{VK}_t[p + \mathsf{OK}_t[p] + 1 + c] + \mathsf{VK}_t[p + c]) \bmod 16$, where the displacement $\delta[p] = \mathsf{OK}_t[p]$ is itself unknown when inverting.

A.4.3 Theorem 1 — Statement

Theorem 1 — One-Use Hidden-Origin Multiplicity.
For any fixed use t, and for any transcript T_t generated by the system from true master keys $(\mathsf{EK}, \mathsf{QK})$, the corresponding hidden origin state S_t is not uniquely determined by T_t. The posterior support on the hidden derivation state contains ≥ 2 consistent hidden origins in the worst case (when $G(\mathsf{VKP}_t)$ has at least one independent odd-length cycle per connected component; $\mu_{\text{odd}} \geq 1$) and ≥ 16 in the non-degenerate case ($\mu_{\text{odd}} = 0$). The exact count is given by the closed-form formula

$$|P(\mathsf{VKC}_t)| = \sum_{\text{compatible } \mathsf{VKP}} \prod_i f(\mu_{i,\text{odd}}(\mathsf{VKP})), \quad f(0) = 16,\ f(k \geq 1) = 2.$$

This bound is algebraic and unconditional — it holds for any adversary including quantum adversaries.

The proof proceeds through dependency graph analysis: spanning tree construction assigns one free anchor variable per connected component (16 choices). Chord (non-tree) edges create cycles; odd-length cycles reduce anchor freedom from 16 to 2 via the equation $2\mathsf{VK}[i_0] \equiv r' \pmod{16}$, which has $\gcd(2, 16) = 2$ and therefore yields exactly 2 solutions when r' is even. Full cycle-case analysis appears in Appendix B.

A.4.4 The [+8] global shift invariant — algebraic engine of the exact coset

The worst-case 2-element ambiguity set has an explicit algebraic source: for all $\mathsf{VK}, \mathsf{OK} \in \mathbb{Z}_{16}^n$,

$$\text{PDAF}_1(\mathsf{VK} + 8 \cdot \mathbf{1}, \mathsf{OK}) = \text{PDAF}_1(\mathsf{VK}, \mathsf{OK})$$

because adding 8 to both positions of any MOD16 sum produces a net shift of $+16 \equiv 0 \pmod{16}$. Therefore $\{\mathsf{EK}, \mathsf{EK} + 8 \cdot \mathbf{1}\}$ permanently produce identical VKC for all VKP_t and all nonces. In the Ideal Configuration, this is an exact result: the coset $\{\mathsf{EK}, \mathsf{EK} + 8 \cdot \mathbf{1}\} \times \{\mathsf{QK}, \mathsf{QK} + 8 \cdot \mathbf{1}\}$ is exactly the set of keys producing identical transcripts for all time.

Correct Placement of [+8].
The [+8] invariant is the algebraic foundation of the exact 4-element ciphertext-equivalent coset in the Ideal Configuration. It is a property of the PDAF_1 function that does not depend on the update dynamics. It establishes Layer 2 unconditionally and, in the Ideal Configuration, produces the exact coset rather than merely a lower bound. EK and $\mathsf{EK} + 8$ produce literally identical ciphertext for every plaintext, every nonce, and every session — they are genuinely, operationally indistinguishable. The equivalent-key objection does not apply: two keys that produce identical ciphertext forever are not two encodings of one key — they are two genuinely distinct keys that the adversary can never separate.

A.4.5 What Layer 2 does and does not establish

Layer 2 establishes: after observing use t, at least 2 hidden origins for S_t are consistent with T_t. Layer 2 does NOT establish: that these alternatives survive unlimited future observation. That is a Layer 4 question. Conflating the two obligations — single-use multiplicity and cross-use non-reduction — is the central structural error the five-layer architecture is designed to avoid.

A.5 Layer 3 — One-Time Non-Reinstantiation (Lemma 2)

A.5.1 The central structural claim

Each message use t generates its hidden derivation state S_t from fixed master secrets $(\mathsf{EK}, \mathsf{QK})$ and fresh per-use public input OR_t unique to use t. The uniqueness of OR_t is guaranteed by $\mathsf{OR_CTR}$ monotonicity combined with CSPRNG randomness.

A.5.2 Lemma 2 — Non-Reinstantiation

Lemma 2 — One-Time Non-Reinstantiation.
For any two distinct uses $t \neq u$, the hidden derivation state S_t is not recreated at use u. Since $\mathsf{OR}_t \neq \mathsf{OR}_u$: $\mathsf{VKP}_t = \mathrm{PDAF}_1(\mathsf{OR}_t, \mathsf{OR}_t)[:n] \neq \mathrm{PDAF}_1(\mathsf{OR}_u, \mathsf{OR}_u)[:n] = \mathsf{VKP}_u$; and $\mathsf{OKP}_t = (\mathsf{VKP}_t + \mathsf{DS_SEP}) \bmod 16 \neq \mathsf{OKP}_u$. Therefore $\mathsf{VKC}_t \neq \mathsf{VKC}_u$ generically. The constraint system induced by T_t over the hidden variables is indexed by $(\mathsf{EK}/\mathsf{QK}, \mathsf{VKP}_t/\mathsf{OKP}_t)$; the constraint system induced by T_u is indexed by a structurally different pair. These are different inversion problems — not the same problem with additional constraints.

A.5.3 Proof of Lemma 2

The injectivity of the map $\mathsf{OR} \mapsto \mathrm{PDAF}_1(\mathsf{OR}, \mathsf{OR})$ — that distinct nonces produce distinct self-expansions — is well-supported by the following structural argument: in the self-referential call, the displacement at each output position is $\delta[p] = \mathsf{OR}[p]$, so the dependency graph $G(\mathsf{OR})$ and the target sum equations both vary simultaneously with OR. This breaks the symmetry that creates preimage collisions in the fixed-OffsetKey case. The displacement indexing and the value indexing change together, making collisions structurally implausible. Exhaustive verification at small n confirms the expected behaviour.

Since VKP is the OffsetKey parameter to PDAF_1, distinct VKP values produce distinct dependency graphs $G(\mathsf{VKP}_t) \neq G(\mathsf{VKP}_u)$. The constraint systems governing the inversion of VKC_t and VKC_u are therefore structurally distinct — different edges, different cycle structures, different target sum parity conditions.

A.5.4 The Phase-5 update complication

Lemma 2 applies directly to fresh-nonce-derived uses. Within a single session, Phase 5 updates the working keys: $\mathsf{VKC}_{\text{next}} = \mathrm{PDAF}_1(\mathsf{OKC}_t, \mathsf{VKP}_t)$ and $\mathsf{OKC}_{\text{next}} = \mathrm{PDAF}_1(\mathsf{VKC}_t, \mathsf{OKP}_t)$. These in-session updates cross-combine VKC_t and OKC_t. This is not a violation of non-reinstantiation in the cross-session sense — different sessions with different OR_t are still independent. In the Ideal Configuration, Phase 5 in-session key updates inherit the [+8] invariant, because the invariant holds for PDAF_1 as a function of its ValueKey argument regardless of the update inputs.

A.6 Layer 4 — No-Later-Information (Theorem 2) — Complete Proof

Layer 4 establishes the no-later-information property for the Ideal Enqpy™ Configuration: future transcript accumulation cannot collapse the hidden-origin ambiguity established in Layer 2. The proof reaches Version C — the strongest form — via a six-step argument that is algebraic, unconditional, and holds for all $n \geq 1$ and all m.

A.6.1 The theorem target

Theorem 2 — No-Later-Information (Target Theorem).
Fix any message use t. Let T_t be the transcript of use t and $T_{>t} = (T_{t+1}, T_{t+2}, \dots)$ be all future transcripts under the same master keys. Theorem 2 establishes: for every transcript prefix $T_{\leq t}$, the conditional distribution of all future transcripts $T_{>t}$ is identical for all four elements of the coset $\{\mathsf{EK}, \mathsf{EK}{+}8\} \times \{\mathsf{QK}, \mathsf{QK}{+}8\}$. No observation of $T_{>t}$, however extended, can distinguish which coset element is the true $(\mathsf{EK}, \mathsf{QK})$. Two formal versions: Version A: $H(\mathsf{EK}, \mathsf{QK} \mid T^{(\infty)}) > 0$ [entropy floor] — PROVED. Version B: $H(\mathsf{EK}, \mathsf{QK} \mid T^{(\infty)}) = \log_2(4) = 2$ bits [exact floor] — PROVED. Version C (strongest): $T_{>t} \perp\!\!\!\perp (\mathsf{EK}, \mathsf{QK}) \mid T_{\leq t}$ [exact conditional independence] — PROVED.

A.6.2 The Ideal Enqpy™ Configuration

The challenge is the Phase 5 cross-combined update. After use t, the system evolves $\mathsf{VKC}_{t+1} = \mathrm{PDAF}_1(\mathsf{OKC}_t, \mathsf{VKP}_t)$. The working keys at use $t+1$ depend on $(\mathsf{OKC}_t, \mathsf{VKP}_t)$. In the Ideal Configuration, $\mathsf{VKP}_t = \mathrm{PDAF}_1(\mathsf{OR}_t, \mathsf{OR}_t)[:n]$ is a function of OR_t alone — it does not depend on EK or QK. $\mathsf{OKC}_t = \mathrm{PDAF}_1(\mathsf{QK}, \mathsf{OKP}_t)$ is part of S_t — but as Step 3 establishes, all four coset elements produce identical OKC_t, so this apparent dependence does not leak distinguishing information.

A.6.3 Proof of Theorem 2 — Six Steps

Step 1 — [+8] Global ValueKey Invariant (algebraic foundation). *Claim:* $\mathrm{PDAF}_1(\mathsf{VK} + 8 \cdot \mathbf{1}, \mathsf{OK}) = \mathrm{PDAF}_1(\mathsf{VK}, \mathsf{OK})$ for all $\mathsf{VK}, \mathsf{OK} \in \mathbb{Z}_{16}^n$ and all $n \geq 1$. *Proof:* The output nibble at position N is $O[N] = (\mathsf{VK}[j_1] + \mathsf{VK}[j_2]) \bmod 16$, where $j_1 = p + c$ and $j_2 = p + \delta + 1 + c$, $\delta = \mathsf{OK}[p]$. Both j_1 and j_2 are determined entirely by OK and N; they do not depend on VK. Replacing VK with $\mathsf{VK} + 8 \cdot \mathbf{1}$ shifts both accessed positions by 8: $O'[N] = (\mathsf{VK}[j_1] + 8 + \mathsf{VK}[j_2] + 8) \bmod 16 = (\mathsf{VK}[j_1] + \mathsf{VK}[j_2] + 16) \bmod 16 = O[N]$. This holds for all N, all OK, and all $n \geq 1$.

Step 2 — Key Role Separation (structural property of Ideal Configuration). *Claim:* In the Ideal Configuration, VKP_t and OKP_t are derived from OR_t alone. Therefore EK does not appear in VKP_t and QK does not appear in OKP_t. *Proof:* By definition, $\mathsf{VKP}_t = \mathrm{PDAF}_1(\mathsf{OR}_t, \mathsf{OR}_t)[:n]$ and $\mathsf{OKP}_t = (\mathsf{VKP}_t + \mathsf{DS_SEP}) \bmod 16$. Both expressions are functions of OR_t only. The index positions j_1 and j_2 selected by the OffsetKey in $\mathrm{PDAF}_1(\mathsf{EK}, \mathsf{VKP}_t)$ are determined by VKP_t alone, which is fixed by OR_t independently of EK. Shifting $\mathsf{EK} \to \mathsf{EK} + 8 \cdot \mathbf{1}$ therefore shifts both accessed positions by the same amount, and Step 1 applies.

Step 3 — VKC and OKC Coset Invariance. From Steps 1 and 2:

$$\mathsf{VKC}_t(\mathsf{EK}{+}8) = \mathrm{PDAF}_1(\mathsf{EK}{+}8, \mathsf{VKP}_t) = \mathrm{PDAF}_1(\mathsf{EK}, \mathsf{VKP}_t) = \mathsf{VKC}_t(\mathsf{EK}),$$
$$\mathsf{OKC}_t(\mathsf{QK}{+}8) = \mathrm{PDAF}_1(\mathsf{QK}{+}8, \mathsf{OKP}_t) = \mathrm{PDAF}_1(\mathsf{QK}, \mathsf{OKP}_t) = \mathsf{OKC}_t(\mathsf{QK}).$$

OKC_t is independent of the EK shift because OKP_t does not depend on EK (Step 2). VKC_t is independent of the QK shift because VKP_t does not depend on QK. Both invariances hold for all OR_t and all n.

Step 4 — Transcript Equivalence for the Full Coset. From Step 3, $\mathsf{CS}_t = \mathrm{PDAF}_1(\mathsf{VKC}_t, \mathsf{OKC}_t)[0..2]$ is identical across the coset. The Selection function therefore applies the same case ordering to the same VKC_t and OKC_t values. $W_t(\mathsf{EK}{+}8, \mathsf{QK}, \mathsf{OR}_t) = W_t(\mathsf{EK}, \mathsf{QK}, \mathsf{OR}_t) = W_t(\mathsf{EK}, \mathsf{QK}{+}8, \mathsf{OR}_t)$. Therefore the ciphertext $C_t = W_t \oplus M_t$ is identical for all four elements of the coset, for every OR_t, and for every M_t. The transcript $T_t = (\mathsf{OR}_t, C_t)$ is identical for all four coset elements at every session.

Step 5 — Conditional Independence (Version C). *Claim:* $T_{>t} \perp\!\!\!\perp (\mathsf{EK}, \mathsf{QK}) \mid T_{\leq t}$. *Proof:* By Step 4, all four coset elements produce identical T_t for every OR_t and every M_t — exact and unconditional. Consider any future session $u > t$ with nonce $\mathsf{OR}_u \neq \mathsf{OR}_t$. All four coset elements produce the same $\mathsf{VKP}_u = \mathrm{PDAF}_1(\mathsf{OR}_u, \mathsf{OR}_u)$ and the same OKP_u (both nonce-derived); Step 3 guarantees VKC_u and OKC_u are identical across the coset; T_u is identical for all four coset elements at every future session $u > t$. Therefore the conditional distribution of $T_{>t}$ given $T_{\leq t}$ is identical for all four coset elements. No observation of $T_{>t}$, however extended, provides any information distinguishing which coset element is the true $(\mathsf{EK}, \mathsf{QK})$.

Step 6 — Exact Equivocation Floor and Coset Tightness. *Floor (2 bits):* Steps 1–5 establish that all four coset elements produce identical transcripts at every session, so $H(\mathsf{EK}, \mathsf{QK} \mid T^{(\infty)}) \geq \log_2(4) = 2$ bits. *Tightness (no larger coset):* For any shift $k \notin \{0, 8\}$, the net output shift is $(\mathsf{VK}[j_1]+k+\mathsf{VK}[j_2]+k) - (\mathsf{VK}[j_1]+\mathsf{VK}[j_2]) = 2k \bmod 16$. This is zero only when $2k \equiv 0 \pmod{16}$, i.e., $k \in \{0, 8\}$. For any other k, the net shift $2k \bmod 16 \neq 0$ applies uniformly at every output position. Transcript equivalence is broken for every $\mathsf{EK} + k \cdot \mathbf{1}$ with $k \notin \{0, 8\}$. Therefore $H(\mathsf{EK}, \mathsf{QK} \mid T^{(\infty)}) = \log_2(4) = 2$ bits exactly. *Phase 5 compatibility:* The in-session key update computes $\mathsf{VKC}_{\text{next}} = \text{PDAF}_1(\mathsf{OKC}_t, \mathsf{VKP}_t)$ and $\mathsf{OKC}_{\text{next}} = \text{PDAF}_1(\mathsf{VKC}_t, \mathsf{OKP}_t)$. By Step 3, all four coset elements produce identical VKC_t and OKC_t; since VKP_t and OKP_t are nonce-derived, all four produce identical $\mathsf{VKC}_{\text{next}}$ and $\mathsf{OKC}_{\text{next}}$. The coset invariance propagates across every Phase 5 update without exception. *Empirical confirmation:* exhaustive search at $n = 4$ over 20 independent sessions finds exactly 4 consistent $(\mathsf{EK}', \mathsf{QK}')$ pairs, corresponding precisely to $\{\mathsf{EK}, \mathsf{EK}{+}8\} \times \{\mathsf{QK}, \mathsf{QK}{+}8\}$. □

QED — Theorem 2, Version C. The Ideal Enqpy™ Configuration satisfies the Shannon Ideal System property unconditionally, with $H(\mathsf{EK}, \mathsf{QK} \mid T^{(\infty)}) = \log_2(4) = 2$ bits exactly.

A.6.4 EnqpyADS™ Variants vs Ideal Configuration — Security Trade-off

The Key Role Separation Principle (§A.6.2) is the condition under which the exact coset-indistinguishability proof above holds for this PDAF_1 construction. *Necessity:* If EK enters the OffsetKey path of any PDAF_1 call, the index positions j_1 and j_2 in Step 3 become functions of EK. Then $\mathsf{EK} \to \mathsf{EK}{+}8$ changes j_1 and j_2, and the Step 1 invariant no longer guarantees output equality. *Sufficiency:* Steps 1–5 above establish that Key Role Separation is sufficient for the full Shannon IS property. *Converse result:* In the HMIX-based standard construction, EK enters OKP derivation. Shifting $\mathsf{EK} \to \mathsf{EK}{+}8$ shifts $\mathsf{OKP}_t \to \mathsf{OKP}_t + 8$ nibble-wise. At $n = 32, 48, 64$, the shift $8 \bmod n \neq 0$, so different index positions are accessed and the coset is broken. EnqpyADS™ variants using HMIX-based or other OffsetKey-coupled derivation carry the Layer 2 per-session equivocation (Theorem 1) but not the global Shannon IS guarantee.

A.7 Layer 5 — Global Shannon Ideal System Corollary

Corollary — Global Shannon Ideal System Property.
For the Ideal Configuration, Theorem 2 is proved (§A.6.3). $H(\mathsf{EK}, \mathsf{QK} \mid T^{(\infty)}) = \log_2(4) = 2$ bits exactly. The adversary does not obtain a unique solution to the hidden key-origin structure even as the number of observed uses tends to infinity. Enqpy™ therefore satisfies Shannon's Ideal System definition as stated in "Communication Theory of Secrecy Systems" (Shannon, 1949): "no matter how much material is intercepted, the enemy still does not obtain a unique solution to the cipher but is left with many alternatives, all of reasonable probability."

A.7.1 Quantum invariance

The Ideal System property is quantum-invariant by construction. The proof across all five layers makes no computational hardness assumption — every step is purely algebraic and unconditional. No quantum speedup — whether quadratic (unstructured search) or exponential (period finding) — can resolve the structural ambiguity that the algebraic proof establishes: all four coset elements remain permanently transcript-indistinguishable regardless of adversarial computational power.

A.8 Equivalent-Key Symmetry vs. Event-Local Irreducible Ambiguity

A.8.1 The distinction

Two fundamentally different mechanisms could produce non-vanishing equivocation:

Case A — Static equivalent-key symmetry: Two keys K and K' produce identical ciphertext behavior for all plaintexts, all nonces, all uses. The "ambiguity" is representational.

Case B — Event-local irreducible ambiguity: Each use creates a one-time derivation event whose hidden origin cannot be determined from that use's transcript alone, and later uses do not revisit the same problem — they instantiate different problems indexed by different nonces.

A.8.2 Which case applies to Enqpy™

The Ideal Enqpy™ Configuration places Enqpy™ squarely in Case B. In the Ideal Configuration, EK and $\mathsf{EK}{+}8$ produce identical PDAF_1 outputs for ALL OffsetKeys and ALL nonces — and this propagates to identical W and identical ciphertext for ALL sessions and ALL plaintexts. This is genuine, permanent, unconditional transcript indistinguishability. The ambiguity is not representational: two distinct keys that produce the same observable output forever are genuinely indistinguishable, not merely differently encoded.

A.8.3 Response to the equivalent-key objection

The critique has two distinct forms:

Form A — Representational objection: "You only proved ciphertext-equivalent key encodings exist. That is a quirk of representation, not meaningful residual secrecy." *Response:* Shannon's Ideal System criterion (1949) is operationally defined: "the enemy is left with many alternative keys of reasonable probability." Shannon's criterion does not require that alternative keys be representationally distinct — only that the adversary faces genuine uncertainty about which key was used. Four keys that produce identical observable output forever constitute exactly this situation.

Form B — Quotient-space objection: "The right object is the quotient key space $\mathcal{K}/\sim$; in that space, the four coset elements collapse to one equivalence class." *Response:* The quotient-space normalization is a modeling choice, not a mathematical fact about the adversary's situation. An adversary who has intercepted ciphertext does not know which coset element was used. Choosing to model the key space as the quotient by the coset does not give the adversary that knowledge — it merely changes the analyst's representation. Shannon's criterion is about the adversary's epistemic state, not the analyst's choice of key-space representation.

A.9 Multi-Observation Stabilization — Strengthened Treatment

A.9.1 The ring-theoretic requirement

A naive formulation — "$m \times n^2$ equations in n unknowns, rank cannot exceed n, therefore stabilization" — imports field-linear-algebra intuition into a non-field ring. $\mathbb{Z}_{16}$ is not a field: it has non-trivial zero divisors (e.g., $2 \times 8 = 0 \bmod 16$). Throughout this section, rank refers to the rank of the presentation matrix of the constraint module, computed via Smith normal form decomposition over $\mathbb{Z}_{16}$.

A.9.2 Strengthened rank argument over $\mathbb{Z}_{16}$

The constraint system for EK given m observations is $\mathrm{PDAF}_1(\mathsf{EK}, \mathsf{VKP}_i) = \mathsf{VKC}_i$ for $i = 1, \ldots, m$. For fixed $(\mathsf{VKP}_i, \mathsf{VKC}_i)$, constraints on EK are nibble-wise linear over $\mathbb{Z}_{16}$ of the form $\mathsf{EK}_t[j_1] + \mathsf{EK}_t[j_2] \equiv r_{j,i} \pmod{16}$ for each edge (j_1, j_2) in $G(\mathsf{VKP}_i)$. As m increases with diverse VKP_i, the solution coset for EK shrinks until it stabilizes at the irreducible coset determined by the global algebraic structure of PDAF_1. The floor is at minimum the $[{+}8]$ 2-element coset, which cannot be eliminated by any constraint from any observation.

A.9.3 The diversity condition

The diversity condition required for rank stabilization is satisfied generically after a single observation: n^2 constraints over n unknowns cover all nibble positions of EK for non-pathological VKP values (those whose dependency graph $G(\mathsf{VKP})$ spans all n nodes, which holds for all but a negligible fraction). The rank ceiling of n is reached at $m = 1$ for such values.

A.10 Proof Boundaries and Explicit Scope

A.10.1 What this proof establishes (unconditionally)

- Layer 1: Formal definitions of all relevant objects — complete and precise.
- Layer 2 (Theorem 1): For any single use, hidden origin of S_t is not uniquely determined by T_t. Lower bound ≥ 2 (worst case) or ≥ 16 (non-degenerate).
- Layer 3 (Lemma 2): S_t is not recreated at any later use.
- Layer 4 (Theorem 2): Proved for Ideal Configuration. $H(\mathsf{EK}, \mathsf{QK} \mid T^{(\infty)}) = 2$ bits exact. Conditional independence $T_{>t} \perp\!\!\!\perp (\mathsf{EK}, \mathsf{QK}) \mid T_{\leq t}$ holds exactly.
- Quantum invariance: all bounds are algebraic and hold against any adversary including quantum adversaries.

A.10.2 Explicit non-claims

- This proof does NOT claim IND-CPA, IND-CCA, or any computational security property.
- This proof (ISP) does not establish plaintext equivocation; that result is in Appendix C.
- This proof does NOT claim resistance to active attacks, nonce-misuse, or key-reuse scenarios beyond what the operational constraints specify.
- This proof does NOT address side-channel attacks, implementation security, or protocol-layer vulnerabilities.

A.10.3 Relationship to Shannon (1949)

Shannon's Ideal System definition requires that no matter how much ciphertext is intercepted, the enemy is left with many alternative keys and plaintexts of reasonable probability. This is formally captured by $H(K \mid C^m, M^m)$ not approaching zero. Enqpy™'s claim maps directly onto this definition under the equivocation-over-raw-keys formalization.

A.11 Summary of Results

Result	Statement	Status
Lemma 1 (MOD16 fiber)	$\lvert F(r)\rvert = 16$ for all $r \in \mathbb{Z}_{16}$. MOD16 is exactly 16-to-1.	Complete (algebraic)
Theorem 1 (one-use mult.)	$\lvert P(\mathsf{VKC}_t)\rvert \geq 2$ (worst case) or ≥ 16 (non-degenerate). Algebraic, unconditional.	Complete (§A.4)
[+8] Invariant (Rem. 6.1)	$\mathrm{PDAF}_1(\mathsf{VK} + 8 \cdot \mathbf{1}, \mathsf{OK}) = \mathrm{PDAF}_1(\mathsf{VK}, \mathsf{OK})$ for all OK, all n. Produces exact 4-element coset $\{\mathsf{EK}, \mathsf{EK}{+}8\} \times \{\mathsf{QK}, \mathsf{QK}{+}8\}$ in Ideal Config.	Complete
Lemma 2 (non-reinst.)	S_t is not recreated at any later use $u > t$.	Complete (structural)
Theorem 2 (no-later-info)	$H(\mathsf{EK}, \mathsf{QK} \mid T^{(\infty)}) = \log_2(4) = 2$ bits exact. $T_{>t} \perp\!\!\!\perp (\mathsf{EK}, \mathsf{QK}) \mid T_{\leq t}$.	Complete (Ideal Config)
Corollary 2 (Shannon IS)	Ideal Config satisfies Shannon's Ideal System unconditionally. Invariant under quantum computation.	Complete
Theorem 3	$H(\mathsf{PT} \mid \mathsf{CT}, \mathsf{OR}) \geq 2n$ bits (worst case; n=64: ≥ 128 bits). See Appendix C.	Complete

Enqpy™ Ideal System Theorem — Rev 1.0 Statement.
Under the Enqpy™ PDAF_SEC construction with HIGH profile parameters ($n = 64$ nibbles, 256-bit keys) and properly generated nonces: (i) The hidden per-use derivation state S_t is not uniquely determined by the transcript of that use (Theorem 1). (ii) S_t is never recreated at any later use (Lemma 2). (iii) No future transcript can resolve which $(\mathsf{EK}, \mathsf{QK})$ generated S_t: $T_{>t} \perp\!\!\!\perp (\mathsf{EK}, \mathsf{QK}) \mid T_{\leq t}$ (Theorem 2). (iv) Therefore $H(\mathsf{EK}, \mathsf{QK} \mid T^{(\infty)}) = \log_2(4) = 2$ bits exactly (Corollary). All results are unconditional with respect to computational resources and are invariant under quantum computation.

Notation and Conventions

Symbol	Definition
$\mathbb{Z}_{16}$	Additive group of integers modulo 16, $\{0, 1, \ldots, 15\}$
n	Key length in nibbles. Min 32 (LOW), 48 (MED), 64 (HIGH)
EK, QK	Master Encryption Key and Query Key $\in \mathbb{Z}_{16}^n$
OR_t	Public nonce for use t (eff_or) — fresh per message
$\mathsf{VKP}_t, \mathsf{OKP}_t$	Per-use working key pointers (nonce-derived; Ideal Config)
$\mathsf{VKC}_t, \mathsf{OKC}_t$	Per-use working key ciphers $= \mathrm{PDAF}_1(\mathsf{EK}, \mathsf{VKP}_t)$ etc.
W_t	Per-use keystream — output of CS-ordered Selection
CS_t	Per-use Case Selector derived from $(\mathsf{VKC}_t, \mathsf{OKC}_t)$
S_t	Hidden per-use derivation state: $(\mathsf{VKC}_t, \mathsf{OKC}_t, \mathsf{CS}_t, W_t)$
$T_t, T^{(m)}, T^{(\infty)}$	Transcripts: per-use, cumulative, infinite
$\mathrm{PDAF}_1(\mathsf{VK}, \mathsf{OK})$	PDAF Mode 1 function $\mathbb{Z}_{16}^n \times \mathbb{Z}_{16}^n \to \mathbb{Z}_{16}^{n^2}$
$G(\mathsf{OK})$	Dependency graph for fixed OK: nodes = VK positions, edges = constraint pairs
$\mu_{\mathrm{odd}}(\mathsf{OK})$	Number of independent odd-length fundamental cycles in $G(\mathsf{OK})$
$c(\mathsf{OK})$	Number of connected components of $G(\mathsf{OK})$
$P(O^*)$	Preimage set: $\{(\mathsf{VK}, \mathsf{OK}) : \mathrm{PDAF}_1(\mathsf{VK}, \mathsf{OK}) = O^*\}$
$H(X \mid Y)$	Conditional Shannon entropy (bits); $\log = \log_2$

B Extended Algebraic Proofs

Enqpy™ Stream Cipher — Extended Algebraic Proofs: Exact Preimage Count, Cycle Case Analysis, and Equivocation Tightness, Rev 1.0 (reproduced in full)

This appendix reproduces in full the Enqpy™ Open Items Closure (OIC Rev 1.0), providing the complete derivation of the exact closed-form preimage count, the rigorous equivocation tightness

proof over $\mathbb{Z}_{16}$, and the full cycle case analysis by induction. Cross-references in the main paper body to "Appendix B, §X" refer to sections within this appendix.

B.1 Exact Preimage Count — Closed-Form Derivation

Theorem 1 establishes $|P(O^*)| \geq 2$ (worst case) for achievable outputs. This section derives the exact closed-form count via spanning-tree decomposition of the dependency graph.

B.1.1 Setup: the dependency graph

Fix an arbitrary OffsetKey $\mathsf{OK} \in \mathbb{Z}_{16}^n$. Define the dependency graph $G(\mathsf{OK})$ as follows: *nodes* are positions $\{0, 1, \ldots, n-1\}$, one per VK nibble; *edges* are defined such that for each output constraint $O^*[N] = (\mathsf{VK}_t[p + \delta[p] + 1 + c] + \mathsf{VK}_t[p + c]) \bmod 16$, there is an undirected edge between the two VK positions referenced (taken mod n to account for tiling).

B.1.2 Rank of the constraint system over $\mathbb{Z}_{16}$

The n^2 constraint equations are of the form $\mathsf{VK}_t[j] + \mathsf{VK}_t[k] \equiv r \pmod{16}$. For a connected graph with V vertices, there is one free anchor variable per component (contributing a factor of 16 to the solution count). For a graph with c connected components, the base solution count per compatible OK is 16^c before odd-length cycle corrections.

B.1.3 Exact closed-form formula

Theorem 1 (extended) — Exact preimage count.
For any achievable output $O^* \in \text{image}(\text{PDAF}_1)$, the exact preimage count is

$$|P(O^*)| = \sum_{\mathsf{OK}\ \text{compatible}} \prod_i f(\mu_{i,\text{odd}}(\mathsf{OK})), \quad f(0) = 16,\ f(k \geq 1) = 2.$$

Here $c(\mathsf{OK})$ is the number of connected components of $G(\mathsf{OK})$, $\mu_{\text{odd}}(\mathsf{OK})$ is the number of independent odd-length cycles in $G(\mathsf{OK})$, and "compatible" means all cycles in $G(\mathsf{OK})$ have even target sums relative to O^*. For each component i, the contribution to the VK solution count is 16 if $\mu_{i,\text{odd}} = 0$, or 2 if $\mu_{i,\text{odd}} \geq 1$; even-length cycles impose only a parity condition on O^* and do not reduce the anchor's 16-fold freedom.

B.1.4 Per-compatible-OK solution count

For any $O^* \in \text{image}(\text{PDAF}_1)$, the corresponding cipher-produced session key (e.g., $\mathsf{VKC} = \text{PDAF}_1(\mathsf{EK}, \mathsf{VKP})$) uses VKP as the OffsetKey. VKP is compatible with VKC by construction — no fraction argument is needed. The VK (i.e., EK) solution count for this compatible OK is determined entirely by the cycle structure of $G(\mathsf{VKP})$:

$$\begin{aligned} |\{\mathsf{EK} : \text{PDAF}_1(\mathsf{EK}, \mathsf{VKP}) = \mathsf{VKC}\}| &= \prod_i f(\mu_{i,\text{odd}}(\mathsf{VKP})) \\ &\geq 2 \quad [\text{worst case: } \mu_{\text{odd}} \geq 1 \text{ per comp.}] \\ &\geq 16 \quad [\text{non-degenerate: } \mu_{\text{odd}} = 0] \end{aligned}$$

B.2 Equivocation Tightness — Rank Argument Over $\mathbb{Z}_{16}$

The Layer 2 algebraic analysis (Theorem 1) establishes $H(\mathsf{EK}, \mathsf{QK} \mid C^m, M^m) \geq 1$ bit for all $m \geq 1$ (worst case). This section proves the floor is stable and non-decreasing.

B.2.1 Combined constraint system rank bound

After m observations, for fixed QK, the EK constraint system has $m \times n^2$ equations in n unknowns. The rank over $\mathbb{Z}_{16}$ cannot exceed n (a system of n unknowns over any commutative ring has at most n independent constraints). For $n = 64$, even $m = 1$ provides 4,096 equations for 64 unknowns. The system is maximally overdetermined after the first observation.

B.2.2 Independence of nonce-derived constraints

Each observation C_i uses pointer key VKP_i derived from a distinct $\mathsf{eff_or}_i$. Two constraints with $\delta_i \neq \delta_j$ reference different EK position pairs for at least one p, making them linearly independent over $\mathbb{Z}_{16}$. Once rank reaches n, further observations cannot increase the rank and the solution space stabilizes at 2 to 16 solutions per compatible VKP:

$$H(\mathsf{EK}, \mathsf{QK} \mid C^m, M^m) \;\to\; [\log_2(2), \log_2(16)] = [1, 4] \text{ bits} \quad \text{as } m \to \infty.$$

Equivocation Tightness Theorem (Layer 2).
For any $m \geq n$, the equivocation has stabilized in the range $[1, 4]$ bits. The floor does not decrease further regardless of additional ciphertext accumulated. For HIGH profile ($n = 64$): equivocation floor $= [1, 4]$ bits, stable for all $m \geq 64$.

B.3 Cycle Case Completeness — $\mathbb{Z}_{16}$ Resolution

B.3.1 The parity condition in context

A cycle of length L in $G(\mathsf{OK})$ gives a system of L equations. Summing all L equations:

$$2 \cdot (\mathsf{VK}[i_0] + \mathsf{VK}[i_1] + \cdots + \mathsf{VK}[i_{L-1}]) \;\equiv\; r_1 + r_2 + \cdots + r_L \pmod{16}. \qquad (\star)$$

B.3.2 Resolution: the structure of multiplication by 2 in $\mathbb{Z}_{16}$

Over $\mathbb{Z}_2$, multiplication by 2 is multiplication by 0, making $(\star)$ degenerate. Over $\mathbb{Z}_{16}$, the image of multiplication by 2 is

$$\mathrm{Im}(\times 2 : \mathbb{Z}_{16} \to \mathbb{Z}_{16}) = \{0, 2, 4, 6, 8, 10, 12, 14\} \quad \text{(even elements of } \mathbb{Z}_{16}).$$

If $\sum r_i$ is even, $(\star)$ is satisfiable. If odd, it has no solution.

B.3.3 Implication for the preimage structure

Lemma 3 — Odd-sum cycles signal image non-membership.
An odd-sum cycle in $G(\mathsf{OK})$ relative to O^* means $O^* \notin \mathrm{image}(\mathrm{PDAF}_1(\cdot, \mathsf{OK}))$. This OK contributes 0 to $|P(O^*)|$. It does not indicate a flaw in the cipher or a reduction of the bound for other OK values.

B.3.4 Compatible OffsetKey fraction (reference result)

For a uniformly random OK, each displacement $\delta[p] = \mathsf{OK}[p]$ is uniform over $\mathbb{Z}_{16}$. Each cycle's target sum is even with probability 1/2. By a parity argument, each independent compatibility constraint is satisfied by exactly 1/2 of uniform-random OKs. In the cipher context, session keys VKC are always produced as $\mathrm{PDAF}_1(\mathsf{EK}, \mathsf{VKP})$, so VKP is always compatible with VKC; the Ideal System proof does not depend on this fraction.

B.4 Exact Lower Bound With Cycles — Induction Proof

This section provides a complete characterization of how cycle length parity determines the exact solution count per connected component.

B.4.1 Cyclomatic number and spanning trees

For a connected graph with V vertices and E edges, the cyclomatic number is $\mu = E - V + 1$. A spanning tree uses $V-1$ edges; the remaining μ edges ("chord" edges) each define one independent cycle. The spanning tree equations, together with one free anchor variable $\mathsf{VK}[i_0]$, uniquely determine all V nibble values. Each chord equation is a constraint on $\mathsf{VK}[i_0]$ whose nature depends on cycle length parity.

B.4.2 Path parity and the anchor coefficient

In the spanning tree, the value of any node j at depth d_j from the anchor i_0 satisfies $\mathsf{VK}[j] = (-1)^{d_j} \cdot \mathsf{VK}[i_0] + c_j \pmod{16}$. For a chord edge connecting nodes j and k with target r, the chord equation becomes

$$\left((-1)^{d_j} + (-1)^{d_k}\right) \cdot \mathsf{VK}[i_0] \;\equiv\; r - c_j - c_k \pmod{16}.$$

The cycle length is $L = d_j + d_k + 1$. The anchor coefficient $a = (-1)^{d_j} + (-1)^{d_k}$ depends on the parity of $d_j + d_k$:

Even-length cycle (L even, $d_j + d_k$ odd): d_j and d_k have different parities. $a = (+1) + (-1) = 0$. The chord equation reduces to $0 \cdot \mathsf{VK}[i_0] \equiv r' \pmod{16}$. This is either always satisfied (all 16 anchor values work) or never (this OK is incompatible with O^*). Even-length cycles do not reduce the solution count.

Odd-length cycle (L odd, $d_j + d_k$ even): d_j and d_k have the same parity. $a = 2$ (both depths even) or $a = -2 \equiv 14 \pmod{16}$ (both depths odd). In both cases $\gcd(a, 16) = 2$, so the chord equation $a \cdot \mathsf{VK}[i_0] \equiv r' \pmod{16}$ has exactly 2 solutions when r' is even (compatible), 0 solutions when r' is odd. The first odd-length cycle reduces the component's anchor from 16 values to 2 values (a factor of 8 reduction).

B.4.3 Theorem 4 — Exact solution count per component

Theorem 4 — Solution count per connected component.
Let $G(\mathsf{OK})$ be the dependency graph for a compatible OK. For each connected component with V_i vertices and $\mu_{i,\text{odd}}$ independent odd-length cycles, the component's contribution to the total solution count is 16 if $\mu_{i,\text{odd}} = 0$, or 2 if $\mu_{i,\text{odd}} \geq 1$. Even-length cycles do not reduce the solution count. Summing over all c connected components: VK solutions for fixed compatible OK $= \prod_i f(\mu_{i,\text{odd}})$ where $f(k) = 16$ if $k = 0$, 2 if $k \geq 1$.

Proof by induction on μ_{odd} within a component. Base case ($\mu_{\text{odd}} = 0$): No odd-length cycles. All chord constraints are even-length (automatically satisfied or signal incompatibility independently of the anchor). The anchor $\mathsf{VK}[i_0]$ has 16 valid choices.

Inductive step ($\mu_{\text{odd}} \to \mu_{\text{odd}} + 1$): Add one odd-length chord edge with even target r'. As established in B.4.2, the chord coefficient a is either 2 or 14; in both cases $\gcd(a, 16) = 2$, so the equation $a \cdot \mathsf{VK}[i_0] \equiv r' \pmod{16}$ restricts $\mathsf{VK}[i_0]$ to exactly 2 values when r' is even. Solution count reduced by factor 8 for the first odd-length chord. Additional odd-length chords impose further constraints on the same 2-element anchor set, leaving exactly 2 solutions if consistent. □

B.4.4 Impact on the entropy bound

For the entropy lower bound on $H(\mathsf{EK} \mid O^*)$ from a single PDAF_1 output, O^* is always achievable — it is a cipher-produced session key. VKP is therefore always compatible with VKC by

construction. No fraction argument is needed:

$$\begin{aligned} H(\mathsf{EK} \mid \mathsf{VKC}, \mathsf{VKP}) &\geq \log_2(f(\mu_{\text{odd}}(\mathsf{VKP}))) \\ &= \log_2(2) = 1 \text{ bit} && [\text{worst case: } \mu_{\text{odd}} \geq 1] \\ &= \log_2(16) = 4 \text{ bits} && [\text{non-degenerate: } \mu_{\text{odd}} = 0] \end{aligned}$$

The worst-case 2-element solution set $\{\mathsf{EK}, \mathsf{EK} + 8 \cdot \mathbf{1}\}$ has a direct algebraic explanation independent of the dependency graph analysis: the [+8] global shift invariant of PDAF_1 is the algebraic generator of the irreducible coset, and is fully consistent with the cycle-parity analysis. An odd-length cycle in $G(\mathsf{VKP})$ forces exactly 2 solutions, and those 2 solutions are precisely the [+8]-coset.

B.5 Summary — Algebraic Results and Relationship to Main Proof

The following results are established in this appendix:

(a) *Exact preimage formula:* $|P(O^*)| = \sum_{\text{compatible } \mathsf{OK}} \prod_i f(\mu_{i,\text{odd}}(\mathsf{OK}))$ [$f(0) = 16$, $f(k \geq 1) = 2$], with per-compatible-OK VK count ≥ 2 worst case and ≥ 16 non-degenerate.

(b) *Equivocation floor:* $H(\mathsf{EK}, \mathsf{QK} \mid C^m, M^m) \geq 1$ bit for all $m \geq 1$, stabilizing at $[1, 4]$ bits.

(c) *Non-vanishing (Layer 2 bound):* $\lim_{m\to\infty} H(\mathsf{EK}, \mathsf{QK} \mid C^m, M^m) \geq 1$ bit > 0. Exact result (Theorem 2, Ideal Configuration): $H(\mathsf{EK}, \mathsf{QK} \mid T^\infty) = \log_2(4) = 2$ bits exactly.

(d) *Quantum invariance:* All bounds are algebraic, requiring no computational hardness assumption, and hold unconditionally against quantum adversaries.

Dual Image Result: The dependency graph $H(\mathsf{VKP})$ analyzed in this appendix also underlies the Plaintext Equivocation Theorem (Appendix C), which establishes the dual result to the Layer 2 preimage count.

C Plaintext Equivocation Theorem

Enqpy™ Stream Cipher — Plaintext Equivocation Theorem, Rev 1.0 (reproduced in full)

This appendix reproduces in full the Enqpy™ Plaintext Equivocation Theorem (PET Rev 1.0), establishing the second axis of the Shannon Ideal System result: $H(\mathsf{PT} \mid \mathsf{CT}, \mathsf{OR}) \geq 128$ bits for HIGH profile ($n = 64$), unconditionally. The proof is independent of and complementary to the key equivocation result of Theorem 2.

C.1 Context and Motivation

C.1.1 The Two-Axis Shannon Ideal System Result

Appendix A establishes the key equivocation theorem: $H(\mathsf{EK}, \mathsf{QK} \mid T^\infty) = \log_2(4) = 2$ bits exactly for the Ideal Configuration. A persistent hostile objection to this result is the equivalent-key argument: the four coset elements $\{\mathsf{EK}, \mathsf{EK}{+}8\} \times \{\mathsf{QK}, \mathsf{QK}{+}8\}$ produce identical ciphertext for every plaintext and every nonce, so they constitute "one effective key encoded four ways" in quotient-space terms.

This appendix establishes an independent second result that is immune to this objection. Even with a single effective key, the adversary faces an astronomically large set of equally probable plaintexts for any observed ciphertext. This is the plaintext axis of Shannon's Ideal System criterion: "the enemy is left with many alternatives, all of reasonable probability."

C.1.2 Empirical Motivation

Over multiple years of cryptanalytic testing, adversaries given only ciphertext (and the public OR) consistently produced credible, structured, legible plaintexts completely different from the actual encrypted content. In 8 of 8 unassisted trials, the adversary found an alternative $(\mathsf{PT}', \mathsf{EK}', \mathsf{QK}')$ tuple consistent with the observed CT. Section C.6 provides the full dataset. These results are empirical confirmations of the Plaintext Equivocation Theorem: for any CT and OR, an exponentially large set of plaintexts — at minimum 2^{128} for HIGH profile — is consistent with CT under some choice of keys.

C.2 Formal Setup

C.2.1 System Model

Under the Ideal Configuration, for fixed nonce OR:

Symbol	Definition
OR	Public per-message nonce, transmitted in clear
VKP	$\mathrm{PDAF}_1(\mathsf{OR}, \mathsf{OR})[:n]$ — public, nonce-derived
OKP	$(\mathsf{VKP} + \mathsf{DS_SEP}) \bmod 16$ — public, nonce-derived
VKC(EK)	$\mathrm{PDAF}_1(\mathsf{EK}, \mathsf{VKP})[:n]$ — hidden, key-derived
OKC(QK)	$\mathrm{PDAF}_1(\mathsf{QK}, \mathsf{OKP})[:n]$ — hidden, key-derived
$W(\mathsf{EK}, \mathsf{QK})$	Selection(VKC, OKC) — per-session keystream
CT	$W \oplus \mathsf{PT}$ — ciphertext
K_{OR}	Keystream function: $(\mathsf{EK}, \mathsf{QK}) \mapsto W(\mathsf{EK}, \mathsf{QK})$
$\mathrm{Im}(K_{\mathsf{OR}})$	$\{W(\mathsf{EK}, \mathsf{QK}) : \mathsf{EK}, \mathsf{QK} \in \mathbb{Z}_{16}^n\}$
$S(\mathsf{CT}, \mathsf{OR})$	$\{\mathsf{PT}' : \exists(\mathsf{EK}', \mathsf{QK}'),\ W(\mathsf{EK}', \mathsf{QK}') \oplus \mathsf{PT}' = \mathsf{CT}\}$

C.2.2 Adversary Model

The adversary is computationally unlimited (information-theoretic). The adversary observes CT and OR (both public). The adversary does not observe EK or QK. The prior over $(\mathsf{EK}, \mathsf{QK})$ is uniform over $\mathbb{Z}_{16}^n \times \mathbb{Z}_{16}^n$. The adversary's goal is to determine PT, or narrow its posterior distribution.

C.2.3 The Dependency Graph $H(\mathsf{VKP})$

Define the functional graph $H(\mathsf{VKP})$ on node set $\{0, \ldots, n-1\}$ with directed edges $p \to q_p$, where

$$q_p = (p + \mathsf{VKP}[p] + 1) \bmod n.$$

$H(\mathsf{VKP})$ has n nodes and n edges (each node has out-degree 1). Every connected component of $H(\mathsf{VKP})$ contains exactly one cycle (the structure of a functional graph). Let $\mu_{\mathrm{odd}}(\mathsf{VKP}) =$ number of components whose cycle has odd length, and $\mu_{\mathrm{even}}(\mathsf{VKP}) =$ number whose cycle has even length.

C.3 The Plaintext Equivocation Theorem

C.3.1 PDAF_1 Restricted Image Size

Theorem 3a — PDAF_1 **Image Size.**
Let $\mathsf{VKP} \in \mathbb{Z}_{16}^n$ be any OffsetKey. Let $H(\mathsf{VKP})$ be its dependency graph with μ_{odd} odd-cycle components and μ_{even} even-cycle components. Then

$$|\mathrm{Im}_{\mathsf{VKP}}| \;:=\; |\{\mathrm{PDAF}_1(\mathsf{EK},\mathsf{VKP})[:n] : \mathsf{EK} \in \mathbb{Z}_{16}^n\}| \;=\; \frac{16^n}{2^{\mu_{\text{odd}}} \cdot 16^{\mu_{\text{even}}}}.$$

Each odd-cycle component introduces a factor-of-2 reduction (mod-2 parity constraint on the cycle's VKC nibbles), and each even-cycle component introduces a factor-of-16 reduction (full mod-16 linear constraint via the telescoping alternating sum). Tree nodes hanging off each cycle contribute freely (factor 16 each). Exhaustive verification at $n = 1, 2, 3, 4$ for all $\mathsf{VKP} \in \mathbb{Z}_{16}^n$ confirms the formula.

C.3.2 Proof of Theorem 3a

The proof proceeds by analyzing the contribution of each connected component of $H(\mathsf{VKP})$ independently.

Step 1 — Component Independence. The PDAF_1 output equation for nibble p is

$$\mathsf{VKC}[p] = \mathsf{EK}[p] + \mathsf{EK}[q_p] \pmod{16}$$

where q_p depends only on $\mathsf{VKP}[p]$. Each connected component of $H(\mathsf{VKP})$ involves a disjoint subset of EK nibble positions. Equations across components share no EK variables. Therefore $|\mathrm{Im}_{\mathsf{VKP}}| = \prod_i (\text{per-component image size})$.

Step 2 — Odd-Cycle Component. Let a component have a cycle of odd length L and T tree nodes. The cycle equations are $\mathsf{VKC}[i] = \mathsf{EK}[i] + \mathsf{EK}[(i+1) \bmod L]$ for $i = 0, \ldots, L-1$. Summing all L equations: $\mathsf{VKC}[0] + \cdots + \mathsf{VKC}[L-1] = 2(\mathsf{EK}[0] + \cdots + \mathsf{EK}[L-1]) \pmod{16}$. The right-hand side is always even. This imposes exactly one mod-2 constraint on the VKC nibbles: their sum must be even. Image contribution from the cycle: $16^L/2$. Each tree node at depth d has $\mathsf{VKC}[t] = \mathsf{EK}[t] + \mathsf{EK}[\text{parent}(t)]$, adding 16 free choices. Total: $(16^L/2) \cdot 16^T$.

Step 3 — Even-Cycle Component. For a cycle of even length L, the telescoping alternating sum gives

$$\mathsf{VKC}[L-1] = \mathsf{VKC}[0] - \mathsf{VKC}[1] + \mathsf{VKC}[2] - \cdots + \mathsf{VKC}[L-2] \pmod{16}.$$

This is one full mod-16 linear constraint. $\mathsf{VKC}[0], \ldots, \mathsf{VKC}[L-2]$ are free ($L-1$ degrees of freedom); $\mathsf{VKC}[L-1]$ is determined. Image contribution from the cycle: 16^{L-1}. Tree nodes contribute 16 each. Total: $16^{L-1} \cdot 16^T$.

Step 4 — Product Formula. Multiplying contributions over all components (the total node count equals n):

$$|\mathrm{Im}_{\mathsf{VKP}}| = \prod_i (\text{cycle_contrib}_i \cdot 16^{T_i}) = \frac{16^n}{2^{\mu_{\text{odd}}} \cdot 16^{\mu_{\text{even}}}}.$$

C.3.3 Coset Structure of the Consistent Plaintext Set

Theorem 3b — Consistent Plaintext Set Structure.
For any CT produced by PDAF_SEC and any OR, defining $\mathsf{VKP} = \mathrm{PDAF}_1(\mathsf{OR}, \mathsf{OR})[:n]$:

$$S(\mathsf{CT}, \mathsf{OR}) = \{\mathsf{CT} \oplus w : w \in \mathrm{Im}(K_{\mathsf{OR}})\}.$$

Therefore: (i) $|S(\mathsf{CT}, \mathsf{OR})| = |\mathrm{Im}(K_{\mathsf{OR}})|$ for all CT — every ciphertext has the same number of consistent plaintexts. (ii) $S(\mathsf{CT}, \mathsf{OR})$ is a coset of $\mathrm{Im}(K_{\mathsf{OR}})$ in the keystream nibble space, shifted by CT. (iii) The achievable plaintext set is independent of the true $(\mathsf{EK}, \mathsf{QK})$ — it depends only on OR.

Proof. $\mathsf{PT}' \in S(\mathsf{CT}, \mathsf{OR}) \iff \exists(\mathsf{EK}', \mathsf{QK}')$: $W(\mathsf{EK}', \mathsf{QK}') \oplus \mathsf{PT}' = \mathsf{CT} \iff W(\mathsf{EK}', \mathsf{QK}') = \mathsf{CT} \oplus \mathsf{PT}' \in \mathrm{Im}(K_{\mathsf{OR}})$. Hence $S(\mathsf{CT}, \mathsf{OR}) = \{\mathsf{CT} \oplus w : w \in \mathrm{Im}(K_{\mathsf{OR}})\}$, which is a coset of $\mathrm{Im}(K_{\mathsf{OR}})$ shifted by CT. Since $\mathrm{Im}(K_{\mathsf{OR}})$ is fixed by OR (not CT), $|S(\mathsf{CT}, \mathsf{OR})| = |\mathrm{Im}(K_{\mathsf{OR}})|$ is constant over CT. □

Lemma 3 — Floor Inheritance.
Let $\mathrm{Im}_{\mathrm{Case}\,1}(K_{\mathsf{OR}}) \subseteq \mathbb{Z}_{16}^{n^2}$ denote the set of keystreams achievable by the Case 1 Selection formula alone ($W[p, C] = \mathsf{OKC}[p] + \mathsf{VKC}[(p + C) \bmod n]$). Since the full PDAF_SEC cipher generates W by selecting from all three cases, every Case 1 achievable keystream is also a full-cipher achievable keystream: $\mathrm{Im}_{\mathrm{Case}\,1}(K_{\mathsf{OR}}) \subseteq \mathrm{Im}(K_{\mathsf{OR}})$. Therefore by set inclusion, $|\mathrm{Im}(K_{\mathsf{OR}})| \geq |\mathrm{Im}_{\mathrm{Case}\,1}(K_{\mathsf{OR}})| \geq 16^{n/2}$. The full-cipher plaintext floor inherits the Case 1 lower bound.

C.3.4 Uniformity of the Posterior

Lemma (Joint Map Uniformity; cf. Lemma 3). The map $(\mathsf{EK}, \mathsf{QK}) \mapsto W_{\mathrm{Case}\,1}$, defined as the composition $(\mathsf{EK}, \mathsf{QK}) \mapsto (\mathsf{VKC}, \mathsf{OKC}) \mapsto W_{\mathrm{Case}\,1}$ via PDAF_1 and Case 1 Selection, is a $\mathbb{Z}_{16}$-module homomorphism from $\mathbb{Z}_{16}^n \times \mathbb{Z}_{16}^n$ to $\mathrm{Im}_{\mathrm{Case}\,1}(K_{\mathsf{OR}})$. All fibers have equal size $16^{2n}/|\mathrm{Im}_{\mathrm{Case}\,1}(K_{\mathsf{OR}})|$.

Proof. Both component maps $\mathsf{EK} \mapsto \mathsf{VKC}$ and $\mathsf{QK} \mapsto \mathsf{OKC}$ are $\mathbb{Z}_{16}$-module homomorphisms (Theorem 3a proof); Case 1 Selection $W_{\mathrm{Case}\,1}[p, C] = \mathsf{OKC}[p] + \mathsf{VKC}[(p + C) \bmod n]$ is linear in both arguments over $(\mathbb{Z}_{16}, +)$; the composition of module homomorphisms is a module homomorphism; equal fiber size follows from the First Isomorphism Theorem. □

Theorem 3c — Uniform Posterior Distribution.
Under a uniform prior over $(\mathsf{EK}, \mathsf{QK}) \in \mathbb{Z}_{16}^n \times \mathbb{Z}_{16}^n$, for any CT and OR:

$$\Pr[\mathsf{PT} = pt \mid \mathsf{CT}, \mathsf{OR}] = \frac{1}{|\mathrm{Im}_{\mathrm{Case}\,1}(K_{\mathsf{OR}})|} \quad \text{for all } pt \in S_{\mathrm{Case}\,1}(\mathsf{CT}, \mathsf{OR}),$$
$$\Pr[\mathsf{PT} = pt \mid \mathsf{CT}, \mathsf{OR}] = 0 \quad \text{for all } pt \notin S_{\mathrm{Case}\,1}(\mathsf{CT}, \mathsf{OR}).$$

The posterior over PT given (CT, OR) is perfectly uniform over the proved Case 1 subset of $S(\mathsf{CT}, \mathsf{OR})$ (extension to full $S(\mathsf{CT}, \mathsf{OR})$ is Conjecture 1). Observing CT provides no information distinguishing among the consistent plaintexts in $S_{\mathrm{Case}\,1}(\mathsf{CT}, \mathsf{OR})$.

Proof of Theorem 3c. The map $\mathsf{EK} \mapsto \mathsf{VKC} = \mathrm{PDAF}_1(\mathsf{EK}, \mathsf{VKP})[:n]$ is a group homomorphism from $(\mathbb{Z}_{16}^n, +)$ to $(\mathbb{Z}_{16}^n, +)$, since the output equations $\mathsf{VKC}[p] = \mathsf{EK}[p] + \mathsf{EK}[q_p]$ are linear over $\mathbb{Z}_{16}$. By the First Isomorphism Theorem for groups, all fibers have equal size: $|\{\mathsf{EK} : \mathrm{PDAF}_1(\mathsf{EK}, \mathsf{VKP})[:n] = v\}| = 16^n/|\mathrm{Im}_{\mathsf{VKP}}|$ for every $v \in \mathrm{Im}_{\mathsf{VKP}}$. For Case 1 Selection specifically, the further map $\mathsf{VKC} \mapsto W_{\mathrm{Case}\,1}$ given by $W_{\mathrm{Case}\,1}[p, C] = \mathsf{OKC}[p] + \mathsf{VKC}[(p + C) \bmod n]$ is linear over $\mathbb{Z}_{16}$ for fixed OKC. The composite $\mathsf{EK} \mapsto \mathsf{VKC} \mapsto W_{\mathrm{Case}\,1}$ is therefore also a group homomorphism, and the First Isomorphism Theorem applies again: all fibers of $\mathsf{EK} \mapsto W_{\mathrm{Case}\,1}$ have equal size. For the QK axis, the argument is symmetric. The joint map $(\mathsf{EK}, \mathsf{QK}) \mapsto W_{\mathrm{Case}\,1}$ is itself a $\mathbb{Z}_{16}$-module homomorphism with constant fiber size over $\mathrm{Im}_{\mathrm{Case}\,1}(K_{\mathsf{OR}})$. □

Conjecture 1 (Full-cipher uniformity): The uniform-fiber property extends to the full three-case $\mathrm{Im}(K_{\mathsf{OR}})$. This is consistent with all empirical evidence (exhaustive verification $n = 2, 3$; 8/8 adversary trials) and holds if the full Selection composition preserves the uniform-fiber property beyond Case 1. Formal algebraic proof of Conjecture 1 for the complete three-case Selection is in progress.

C.4 Minimum Consistent Plaintext Set Size

C.4.1 Worst-Case VKP Analysis

The minimum $|\mathrm{Im}(K_{\mathsf{OR}})|$ over all possible OR determines the unconditional lower bound on plaintext equivocation. Minimizing $|\mathrm{Im}_{\mathsf{VKP}}|$ requires maximizing the denominator $2^{\mu_{\text{odd}}} \cdot 16^{\mu_{\text{even}}}$. Since each factor of 16 in the denominator reduces the image more than a factor of 2, the minimum is achieved by maximizing μ_{even}. The maximum is $n/2$ (all nodes in 2-cycles). Then $\mu_{\text{even}} = n/2$, $\mu_{\text{odd}} = 0$, and

$$|\mathrm{Im}_{\mathsf{VKP}}|_{\min} = \frac{16^n}{16^{n/2}} = 16^{n/2}.$$

C.4.2 Security Profile Table

Profile (n)	**Minimum** $\lvert S(\mathsf{CT}, \mathsf{OR})\rvert$
LOW ($n = 32$, 128-bit)	$16^{16} = 2^{64} \approx 1.8 \times 10^{19}$ consistent plaintexts
MEDIUM ($n = 48$, 192-bit)	$16^{24} = 2^{96} \approx 7.9 \times 10^{28}$ consistent plaintexts
HIGH ($n = 64$, 256-bit)	$16^{32} = 2^{128} \approx 3.4 \times 10^{38}$ consistent plaintexts

For the HIGH profile, the minimum plaintext set size 2^{128} matches the NIST quantum security target for 256-bit keys. The adversary faces at least 2^{128} consistent plaintext alternatives for any observed ciphertext, in the absolute worst case over all possible nonces.

C.4.3 Shannon's Criterion — Direct Satisfaction

Shannon's Equivocation Criteria — Satisfied on Both Axes.

Shannon (1949): "The enemy does not obtain a unique solution to the cipher but is left with many alternatives, all of reasonable probability."

Axis 1 (Key Equivocation, proved in Appendix A): $H(\mathsf{EK}, \mathsf{QK} \mid T^{\infty}) = 2$ bits exactly. Four alternative key pairs are permanently consistent with any transcript. Objection: "these are the same effective key" (equivalent-key / quotient-space).

Axis 2 (Plaintext Equivocation, proved in this appendix): $H(\mathsf{PT} \mid \mathsf{CT}, \mathsf{OR}) \geq 128$ bits (HIGH profile, worst case). At least 2^{128} alternative plaintexts are consistent with any ciphertext. Immune to equivalent-key objection: the message ambiguity is independent of key normalization.

Together: the adversary who observes $(\mathsf{CT}, \mathsf{OR})$ cannot determine either the key OR the message. Shannon's criterion is met on both axes simultaneously.

C.5 Multi-Session Stability

C.5.1 Non-Reinstantiation Ensures Per-Session Independence

Lemma 2 (Non-Reinstantiation) establishes that different sessions use different nonces OR_t, producing different VKP_t values and hence structurally independent constraint systems. Cross-session observations cannot resolve the plaintext ambiguity of any single session. Formally: for each session t, $S(\mathsf{CT}_t, \mathsf{OR}_t)$ is determined by $\mathrm{Im}(K_{\mathsf{OR}_t})$, which depends only on $\mathsf{VKP}_t = \mathrm{PDAF}_1(\mathsf{OR}_t, \mathsf{OR}_t)[:n]$. Since $\mathsf{VKP}_t \neq \mathsf{VKP}_u$ for $t \neq u$, the achievable keystream sets for different sessions are indexed by different dependency graphs.

Corollary — Multi-Session Plaintext Equivocation.
For any session t and any transcript $T^\infty = (\mathsf{CT}_1, \mathsf{OR}_1, \mathsf{CT}_2, \mathsf{OR}_2, \dots)$:

$$H(\mathsf{PT}_t \mid T^\infty) \;\geq\; H(\mathsf{PT}_t \mid \mathsf{CT}_t, \mathsf{OR}_t) \;\geq\; 2n \text{ bits} \quad \text{(worst case)}.$$

Unlimited transcript accumulation does not reduce the plaintext equivocation below the per-session floor. The message ambiguity is permanent and stable.

C.6 Empirical Confirmation — Cryptanalyst Results

C.6.1 Experimental Design

Ten ciphertexts were produced using PDAF_SEC under the Ideal Configuration with HIGH profile parameters ($n = 64$). An adversary was provided only the ciphertext file and the public OR values. No keys were provided. Results from 8 unassisted trials and 2 hint-assisted trials are reported.

C.6.2 Results

Trial	Outcome
#1 (unassisted)	Adversary produced: English sentence about WhatsApp. True PT: English sentence about quantum effort. WRONG — confirms theorem.
#2 (unassisted)	Adversary produced: WhatsApp company culture text. True PT: Tim Cook quotation. WRONG.
#3 (unassisted)	Adversary produced: English text about funding. True PT: BASE64-like random string. WRONG. TRUE PT IS NOT NATURAL LANGUAGE — strongest confirmation.
#4 (PT given)	Adversary reproduced correct PT. Also asked to recover EK/QK from (CT, OR, PT): COULD NOT. Confirms one-way gate.
#5 (unassisted)	Adversary produced: separator text. True PT: romantic sentence. WRONG.
#6 (URL hinted)	Adversary found correct URL after being told to look for a specific YouTube video. Confirms underdetermination.
#7 (unassisted)	Adversary produced: English sentence. True PT: DKIM email header. WRONG. TRUE PT IS NOT NATURAL LANGUAGE.
#8 (unassisted)	Adversary produced: English paragraphs. True PT: raw binary string of 1s and 0s. WRONG. TRUE PT IS BINARY DATA.
#9 (unassisted)	Adversary produced: table header text. True PT: Vin Scully quotation. WRONG.
#10 (unassisted)	Adversary produced: English sentence. True PT: VB error code. WRONG. TRUE PT IS CODE.

Trials #3, #7, #8, and #10 are the most significant: the true plaintexts are not natural language (random string, email header, binary data, program code), yet the adversary produced fluent English paragraphs. This confirms that the achievable plaintext set for any ciphertext contains multiple semantic categories including natural language, structured data, binary content, and code — exactly as Theorem 3b predicts.

C.6.3 Interpretation

Each adversary result is an empirical demonstration that an alternative $(\mathsf{PT}', \mathsf{EK}', \mathsf{QK}')$ tuple exists satisfying $\mathsf{PDAF_SEC}(\mathsf{EK}', \mathsf{QK}', \mathsf{OR}, \mathsf{PT}') = \mathsf{CT}$. The adversary cannot determine which plaintext is the true one. This is not a cryptographic break — it is Theorem 3b confirmed experimentally. The results in this section are illustrative only. No proof step in §C.3–C.5 relies on empirical evidence; all proofs are algebraic and unconditional.

C.7 Relationship to Existing Proof Structure

C.7.1 Dual of the Layer 2 Preimage Theorem

The Layer 2 preimage theorem (Theorem 1, Appendix B) establishes $|\{\mathsf{EK} : \mathrm{PDAF}_1(\mathsf{EK}, \mathsf{VKP})[:n] = \mathsf{VKC}\}| \geq 2$ (worst case). This counts how many EK values produce the same VKC — the preimage multiplicity. The Image Size Theorem 3a is the dual result: it counts how many VKC values are achievable at all. The two quantities are related by

$$|\mathrm{Im}_{\mathsf{VKP}}| \cdot |\text{preimage(any VKC)}| = 16^n,$$

since the preimage sizes are uniform (Theorem 3c). This provides a consistency check: the Layer 2 preimage lower bound of 2 corresponds to an image upper bound of $16^n/2$, confirming that the image reduction in Theorem 3a is tight.

C.7.2 Five-Layer Architecture — Extended

Layer	Theorem
Layer 1	Formal System Model — definitions of S_t, T_t, K_{OR} (Appendix A)
Layer 2 / Thm. 1	Preimage multiplicity: $\lvert\{\mathsf{EK} : \mathrm{PDAF}_1(\mathsf{EK}, \mathsf{VKP}) = \mathsf{VKC}\}\rvert \geq 2$ (Appendix A, B)
Layer 3 / Lem. 2	Non-Reinstantiation: S_t never recreated at any later use (Appendix A)
Layer 4 / Thm. 2	Key equivocation: $H(\mathsf{EK}, \mathsf{QK} \mid T^\infty) = 2$ bits, Ideal Config (Appendix A)
Layer 5 / Cor.	Shannon IS property: key axis satisfied (Appendix A)
New: Thm. 3	Plaintext equivocation: $H(\mathsf{PT} \mid \mathsf{CT}, \mathsf{OR}) \geq 128$ bits ($n = 64$) (this appendix)
New: Cor.	Shannon IS property: message axis satisfied — immune to equivalent-key objection

C.8 Proof Obligations and Status

Obligation	Status
(A) Image size formula $\lvert\mathrm{Im}_{\mathsf{VKP}}\rvert = 16^n/(2^{\mu_{\text{odd}}} \cdot 16^{\mu_{\text{even}}})$	Proved — §C.3.2; verified exhaustively $n = 1..4$
(B) Minimum $\lvert\mathrm{Im}_{\mathsf{VKP}}\rvert = 16^{n/2}$ over all VKP	Proved — §C.4.1
(C) $\lvert\mathrm{Im}_{\mathsf{VKP}}\rvert$ grows as $16^{n/2}$ with n (exponential)	Proved — follows directly from formula
(D) Posterior uniformity: $\lvert K_{\mathsf{OR}}^{-1}(w)\rvert$ constant over $\mathrm{Im}(K_{\mathsf{OR}})$	Proved for $\mathrm{Im}_{\text{Case 1}}(K_{\mathsf{OR}})$ — group homomorphism argument; verified $n = 2, 3$ exhaustively. Conjectured to extend to full $\mathrm{Im}(K_{\mathsf{OR}})$; see Conjecture 1.
(E) Multi-session stability: $H(\mathsf{PT}_t \mid T^\infty) \geq H(\mathsf{PT}_t \mid \mathsf{CT}_t, \mathsf{OR}_t)$	Proved — follows from Lemma 2
(F) Full algebraic characterization of $\mathrm{Im}(K_{\mathsf{OR}})$ across all three Selection cases	Lower bound PROVED (Case 1 alone suffices). Full algebraic characterization of the combined three-case image is in progress.

Obligation (F) is a full-characterization question, not a validity question about the proved floor. The lower bound $|S(\mathsf{CT}, \mathsf{OR})| \geq 16^{n/2}$ is proved unconditionally from Case 1 alone. Cases 2 and 3 of the Selection phase can only ADD achievable keystreams beyond those reachable via Case 1. Therefore the proved floor $16^{n/2}$ is a valid, unconditional lower bound on the full cipher's achievable plaintext set.

C.9 Summary of Results

Result	Statement
Theorem 3a (Image Size)	$\lvert\mathrm{Im}_{\mathsf{VKP}}\rvert = 16^n/(2^{\mu_{\mathrm{odd}}} \cdot 16^{\mu_{\mathrm{even}}})$. Verified exhaustively $n = 1..4$.
Theorem 3b (Coset)	$\lvert S(\mathsf{CT}, \mathsf{OR})\rvert = \lvert\mathrm{Im}(K_{\mathsf{OR}})\rvert$ for all CT.
Theorem 3c (Uniformity)	$\Pr[\mathsf{PT} = pt \mid \mathsf{CT}, \mathsf{OR}] = 1/\lvert\mathrm{Im}_{\mathrm{Case\,1}}(K_{\mathsf{OR}})\rvert$ over Case 1 subset.
Minimum Floor	$\lvert S(\mathsf{CT}, \mathsf{OR})\rvert \geq 16^{n/2}$. For $n = 64$: $\geq 2^{128}$.
Entropy Statement	$H(\mathsf{PT} \mid \mathsf{CT}, \mathsf{OR}) \geq 4(n/2) = 2n$ bits. For $n = 64$: ≥ 128 bits.
Multi-session	$H(\mathsf{PT}_t \mid T^\infty) \geq 2n$ bits.
Shannon Alignment	Directly satisfies "many alternatives, all of reasonable probability" — message axis.
Quotient-Space Stable	Message ambiguity is independent of key normalization.

Enqpy™ Plaintext Equivocation Theorem — Rev 1.0 Statement.

Under the Enqpy™ PDAF_SEC construction with HIGH profile parameters ($n = 64$) and properly generated nonces:

• For any ciphertext CT and any public nonce OR, the set of plaintexts consistent with $(\mathsf{CT}, \mathsf{OR})$ under some choice of master keys has size at least 2^{128}.

• All elements of the proved Case 1 achievable subset are equally probable under a uniform key prior (Theorem 3c). Extension of this uniformity to the full achievable set is Conjecture 1.

• Unlimited transcript accumulation does not reduce this plaintext ambiguity.

• This result is unconditional, quantum-invariant, and independent of the equivalent-key objection applicable to the key equivocation result.

Together with $H(\mathsf{EK}, \mathsf{QK} \mid T^\infty) = 2$ bits (Appendix A), the Enqpy™ construction satisfies Shannon's equivocation criteria — permanent, non-vanishing key equivocation (2 bits exact) and exponential plaintext equivocation ($\geq 2^{128}$ consistent plaintexts, HIGH profile) — on both axes simultaneously, under the Ideal Configuration.